FÖRSVARSMAKTEN

Handbok Säkerhetstjänst Informationssäkerhet

2013

Handbok
Försvarsmaktens säkerhetstjänst, Informationssäkerhet

H Säk Infosäk 2013

Omslagsbild: Anna-Karin Wetzig, FMV-FSV Grafisk produktion Stockholm 2014

Grafisk bearbetning och tryck: FMV-FSV Grafisk produktion, Stockholm
Produktions-ID: 130618-001
Produktionsformat: G5 InDesign. Ändring nr 2 är införd i PDF.

Publikationsområde: H SÄK Infosäk

M-nr: M7739-352056

FÖRSVARSMAKTEN

Datum	HKV beteckning
2013-06-26	10 440:59810

Handbok för Försvarsmaktens säkerhetstjänst, Informationssäkerhet (H SÄK Infosäk), 2013 års utgåva (M7739-352056) fastställs för tillämpning fr.o.m. 2013-09-02.

Målgruppen är främst säkerhetschefer och IT-säkerhetschefer samt annan personal som arbetar med informationssäkerhetsfrågor. Handboken gäller för Försvarsmakten. Andra myndigheter inom Försvarsmaktens tillsynsområde för säkerhetsskydd (t.ex. Försvarets radioanstalt och Försvarets materielverk) kan även i tillämpliga delar använda den i sitt arbete med informationssäkerhet.

Därmed upphävs:
- Kapitel 3 och 4 i handbok för Försvarsmaktens säkerhetstjänst, Säkerhetsskyddstjänst (H SÄK Skydd) 2007 års utgåva (M7739-352005).
- Handbok för Försvarsmaktens säkerhetstjänst, Informationsteknik (H SÄK IT), 2006 års utgåva med ändring 1, 2008, M7745-734062.
- Riktlinjer för klassificering av olika former av handlingar (HKV 2008-06-25 10 812:72264).
- Kommentarer till bl.a. Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar (HKV 2011-03 -10 10 700:52814) vad avser:
  - o Bilaga 1: 1 kap. 1-3, 8-10 och 12-14 §§, 2 kap. 2-5 och 8 §§, 3 kap. 1-9 §§ samt 4 kap. 1 §.
  - o Bilaga 2: 2 kap. 2 a § och 9 kap. 2 och 5 a §§.
  - o Bilaga 3.

I arbetet med handboken har främst Kim Hakkarainen, kapten Stefan Styrenius, Ann-Marie Löf och avdelningsdirektör Zenobia Rosander deltagit.

I avvaktan på att handboken produceras i tryckt form tillgängliggörs den som PDF. I samband med att handboken kommer ut i tryckt form ges en ny PDF ut på emilia.

Chefen för säkerhetskontoret vid militära underrättelse- och säkerhetstjänsten får fatta beslut om ändringar i handboken inom ramen för 2013 års utgåva. Beslut i detta ärende har fattats av generalmajor Gunnar Karlson. I den slutliga handläggningen har deltagit överste Mattias Hanson, överstelöjtnant Patrik Lind samt, som föredragande, kapten Stefan Styrenius, Ann-Marie Löf och avdelningsdirektör Zenobia Rosander.

Gunnar Karlson
Chef för militära underrättelse- och säkerhetstjänsten

Stefan Styrenius | Ann-Marie Löf | Zenobia Rosander

Revidering - ändringslogg

Nr	Sida	Omfattning	Datum föredragning Beslut av	VIDAR ärende nr
1		Omfattning Kapitel 11 om åtgärder vid förlust och röjande av uppgift eller handling har ändrats. Handboken har även ändrats med hänsyn till Försvarsmaktens föreskrifter (FFS 2013:4) med arbetsordning för Försvarsmakten (FM ArbO). Väsentliga ändringar i handboken är markerade genom kantstreck. Ändringar som rör stavning, numrering på fotnoter och referenser är inte markerade med kantstreck.	17/6 2014 Beslut av överste Mattias Hanson	FM2014-5468:1
2		Kapitel 11 ersatt av H Säk men 2017	2017-05-19, C MUST	FM2014-5468:2

Sida avser sidnummer i den rättade versionen.
Ändringar i texten framgår av ändringsmarkör.

Kom ihåg!

Om du läser denna publikation i pappersform – kontrollera att du har den senaste utgåvan. Fastställd och gällande utgåva finns alltid på Försvarsmaktens intranät.

Förord

Information är ofta en förutsättning för att Försvarsmakten ska kunna lösa sina uppgifter. Den militärstrategiska doktrinen för Försvarsmakten innebär att vi för en motståndare ska kunna undanhålla information om vår faktiska förmåga, våra avsikter och vårt kunskapsläge om omvärlden. Informationssäkerhet är en förutsättning för krigföring.

Nödvändigheten av att skydda Försvarsmaktens information varierar emellertid för olika typer av information och skeden. Vissa förberedelser i fred behöver skyddas under lång tid. I taktiska situationer kan information ha en kort bäst före-tid, och behovet att skydda informationen vara mer begränsad. Informationssäkerhet är också en gemensam angelägenhet när Försvarsmakten löser uppgifter tillsammans med andra stater, t.ex. inom ramen för internationella militära insatser. Det gäller också när vi samverkar med andra myndigheter i Sverige. Informationssäkerhet är en förutsättning för förtroende som gör det möjligt att utbyta information med våra samarbetspartner.

En effektiv hantering av information innebär att den hanteras i elektronisk form. Sverige har under flera år haft en topposition i internationella undersökningar om IT. Användningen av IT är omfattande i Sverige, vårt samhälle har lätt att ta till sig nya produkter och tjänster. Det är lätt att bli överväldigad av de nya möjligheterna och använda dessa utan att i förväg ha övervägt vilka hot som den nya IT-användningen medför. Det är därför på sin plats att vara försiktig så att vi inte utsätter våra informationstillgångar för okända eller oacceptabla risker. Samtidigt får inte försiktigheten medföra att vi onödigtvis avstår från att effektivt hantera våra informationstillgångar med IT, t.ex. för information med lågt skyddsvärde. Vårt beroende av IT medför att vi behöver uppmärksamma tillgänglighets- och riktighetsaspekterna mer än vad vi tidigare har gjort. Traditionellt har informationssäkerhet i Försvarsmakten varit ensidigt fokuserad på sekretessaspekten.

Denna handbok vänder sig mer till dig som direkt ska stödja Försvarsmaktens informationssäkerhetsarbete än till anställda som hanterar informationstillgångarna. De anställdas informations- och utbildningsbehov tillgodoses med andra medel. Handboken ska läsas tillsammans med de övriga handböckerna i Försvarsmaktens säkerhetstjänst.

Gunnar Karlson
Chef för militära underrättelse- och säkerhetstjänsten

Läsanvisning

Handboken innehåller förklarande text till de författningar som reglerar informationssäkerheten i Försvarsmakten. Handboken innehåller också Försvarsmaktens uppfattning om hur föreskrifter om säkerhetsskydd ska tillämpas vid en myndighet som Försvarsmakten har föreskriftsrätt över vad gäller säkerhetsskydd.[1] En sådan uppfattning anges när *myndighet* finns i en text under en föreskrift ur säkerhetsskyddslagen (1996:627), säkerhetsskyddsförordningen (1996:633) och Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd. Om det inte står något annat avser myndighet en svensk myndighet.

Text ur en myndighets föreskrifter och Försvarsmaktens interna bestämmelser återges i beige rutor med *kursiv stil*. Författningstext ur lagar och förordningar återges i beige rutor med ***fet kursiv stil***.

När *ska* används i löpande text i fråga om ett krav är det med stöd av en föreskrift till vilken hänvisning sker med fotnot. De råd, riktlinjer och rekommendationer som anges i denna handbok bör i Försvarsmakten alltid följas om inte särskilda skäl föreligger att genomföra verksamheten på annat sätt. När *bör* används i löpande text är det således Försvarsmaktens uppfattning i frågan.

Med *OSL* avses offentlighets- och sekretesslagen (2009:400). Med *OSF* avses offentlighets- och sekretessförordningen (2009:641). Med *TF* avses tryckfrihetsförordningen. Med *YGL* avses yttrandefrihetsgrundlagen.

I handboken görs hänvisningar till bl.a. Försvarsmaktens interna bestämmelser (FIB 2007:2) om säkerhetsskydd och skydd av viss materiel samt Försvarsmaktens interna bestämmelser (FIB 2006:2) om IT-säkerhet. Försvarsmaktens interna bestämmelser om säkerhet och skydd av viss materiel har ändrats genom FIB 2010:1 och FIB 2010:5. Försvarsmaktens interna bestämmelser om IT-säkerhet har ändrats genom FIB 2010:2, FIB 2010:6 och FIB 2011:1. FIB 2010:1 och FIB 2010:2 utgör även omtryck av författningarna. Vid hänvisning till någon av dessa ändrade författningar används dock den ursprungliga författningsbeteckningen; nämligen FIB 2007:2 respektive FIB 2006:2.

Föreskrifter som rör skydd för utrikes- och sekretessklassificerade uppgifter och handlingar gäller endast i Försvarsmakten.

I handboken anges författningarna endast med rubrik. I bilaga 1 återfinns de författningar med författningsbeteckning som anges i denna handbok.

1 11 § andra stycket och 44 § säkerhetsskyddsförordningen.

Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen genom utlämnande av en allmän handling eller på något annat sätt.[2] Med *hemlig uppgift* avses i denna handbok en uppgift som omfattas av sekretess enligt OSL och som rör rikets säkerhet. Med *hemlig handling* avses i denna handbok en handling som innehåller hemlig uppgift.[3] Med hemlig handling förstås alltså en handling, vare sig den är allmän eller inte. Med *kvalificerat hemlig uppgift* avses i denna handbok en uppgift som omfattas av sekretess enligt offentlighets- och sekretesslagen och som är av synnerlig betydelse för rikets säkerhet. En *kvalificerat hemlig handling* är en handling som innehåller en kvalificerat hemlig uppgift.

I handboken återfinns exemplen i gula rutor samt i löptext. En ofärgad ruta används för ett särskilt påpekande för text som inte är en föreskrift eller ett exempel.

Referenser till bl.a. skrivelser i Försvarsmakten anges med hakparenteser, t.ex. [referens 1]. Bilaga 2 innehåller en förteckning över de refererade dokumenten.

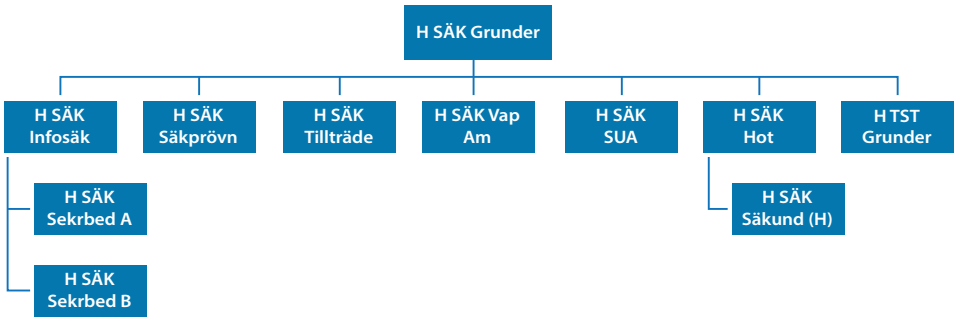
Produktionschefen ska leda och samordna IS/IT-området inom Försvarsmakten.[4] Försvarsmaktens IT-styrmodell beskrivs i avsnitt 2.3.

Med *organisationsenhet* avses Högkvarteret samt förband, skolor och centrum, vilka är angivna som organisationsenheter i förordningen (2007:1266) med instruktion för Försvarsmakten. Med *MUST* avses militära underrättelse- och säkerhetstjänsten i Högkvarteret. Med *expedition* avses även registratur eller motsvarande funktion som svarar för registrering av allmänna handlingar vid en myndighet.

Bilaga 6 innehåller en begreppsförklaring. För begrepp som hör till den militära säkerhetstjänstens organisation och verksamhet hänvisas till Handbok för Försvarsmaktens säkerhetstjänst Grunder (H SÄK Grunder).

För redaktionella ändringar i handboken, se uppdaterade version av handboken på säkerhetstjänstens portal i Försvarsmaktens intranät.

2 3 kap. 1 § OSL.
3 4 § 1 och 2 säkerhetsskyddsförordningen.
4 9 kap. 8 § 2 Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).



Utöver H SÄK Infosäk omfattar den militära säkerhetstjänstens handböcker:

- H SÄK Grunder – grunderna för den militära säkerhetstjänsten inklusive säkerhetsplanering, utbildning, kontrollverksamhet och internationell verksamhet.
- H SÄK Sekrbed A – grunderna vad avser klassificering av information inklusive sekretessbedömning och inplacering av uppgifter i informationssäkerhetsklass.
- H SÄK Sekrbed B – råd och riktlinjer för ämnesvis klassificering av information.
- H SÄK Säkprövning – grunderna vad avser säkerhetsprövning.
- H SÄK Tillträde – grunderna vad avser tillträdesbegränsning.
- H SÄK Vap Am – grunderna vad avser hantering av vapen och ammunition.
- H SÄK SUA – grunderna vad avser säkerhetsskyddad upphandling med säkerhetsskyddsavtal.
- H SÄK Hot – grunderna vad avser säkerhetshotande verksamhet.
- H SÄK Säkund (hemlig) – grunderna vad avser säkerhetsunderrättelsetjänst.
- H TST Grunder – grunderna vad avser signalskyddstjänst.

Innehåll

Bild och illustrationsförteckning

ILLUSTRATION	ILLUSTRATÖR	SIDNR	NOT
Omslagsbild	Anna-Karin Wetzig/FMV-FSV-APS Grafisk produktion		
Bild 9:1, 12:2, 13:4	Kjell Ström/Försvarsmakten	85, 207, 242	
Bild 9:19	Försvarsmakten	146	Bild hämtad från H SÄK Skydd 2007
Bild 12:1	Anna-Karin Wetzig/FMV-FSV-APS Grafisk produktion	206	
Bild 12:2	Kjell Ström/Försvarsmakten	207	
Bild 12:5	Kim Hakkarainen/Försvarsmakten	223	
Bild 12:7	Kim Hakkarainen/Försvarsmakten	228	
Bild 12:8	Kim Hakkarainen/Försvarsmakten	230	
Bild 13:2	Kim Hakkarainen/Försvarsmakten	236	
Bild 13:4	Kjell Ström/Försvarsmakten	242	

FOTO	FOTOGRAF	SIDNR	NOT
Foto 9:22	Försvarsmakten	177	
Foto 9:23	Försvarsmakten	178	
Foto 12:3	Kim Hakkarainen/Försvarsmakten	214	
Foto 12:4	Kim Hakkarainen/Försvarsmakten	214	

1 Informationssäkerhet

Informationssäkerhet kan sägas vara administrativa och tekniska skyddsåtgärder som anpassas efter informationstillgångarnas betydelse. Informationssäkerhet brukar vanligtvis avse aspekterna konfidentialitet, riktighet och tillgänglighet samt spårbarhet. Sekretess enligt OSL är ett exempel på författningskrav på konfidentialitet.

Behov av informationssäkerhet skiftar för olika verksamheter i samhället och vilka typer av informationstillgångar som förekommer. Samhällets informationssäkerhet som avser skyddet för hemliga uppgifter har en särställning med långtgående författningskrav för att bl.a. förebygga att sådana uppgifter obehörigen röjs.

Även andra typer av informationstillgångar behöver omfattas av informationssäkerhet, utan att omfattas av ett säkerhetsskydd. Vad informationssäkerhet är i Försvarsmakten beskrivs i avsnitt 2.1 om Försvarsmaktens informationssäkerhetspolicy.

Bild 1:1 - *Informationssäkerheten är beroende av människor, administration och teknik.*

Skyddsåtgärderna som ska uppnå den önskade informationssäkerheten kan sällan utföras utan att hänsyn tas till *tekniken* som ska användas eller som det finns ett beroende till, *administration* samt de *människor* som hanterar informationstillgångarna eller skyddsåtgärderna (bild 1:1).

Med *administration* avses här t.ex. organisation och rutiner. Ett exempel är behörighetsstyrning i ett IT-system där behörighetsstyrningen inte enbart kan utgöras av en teknisk funktion utan även kräver rutiner för styrningen och människor som t.ex. beslutar och genomför konfiguration av den tekniska funktionen så att behörighetsstyrningen får avsedd effekt. Även om en skyddsåtgärd till sin karaktär är teknisk omfattar den således även administrativa delar.

Bild 1:2 visar schematiskt hur informationssäkerheten kan uppnås genom olika administrativa och tekniska skyddsåtgärder. Ansvaret för ledning, genomförande och utvärdering av de olika skyddsåtgärderna kan finnas vid flera enheter inom en myndighet men syftar gemensamt till att uppnå myndighetens mål med informationssäkerheten.

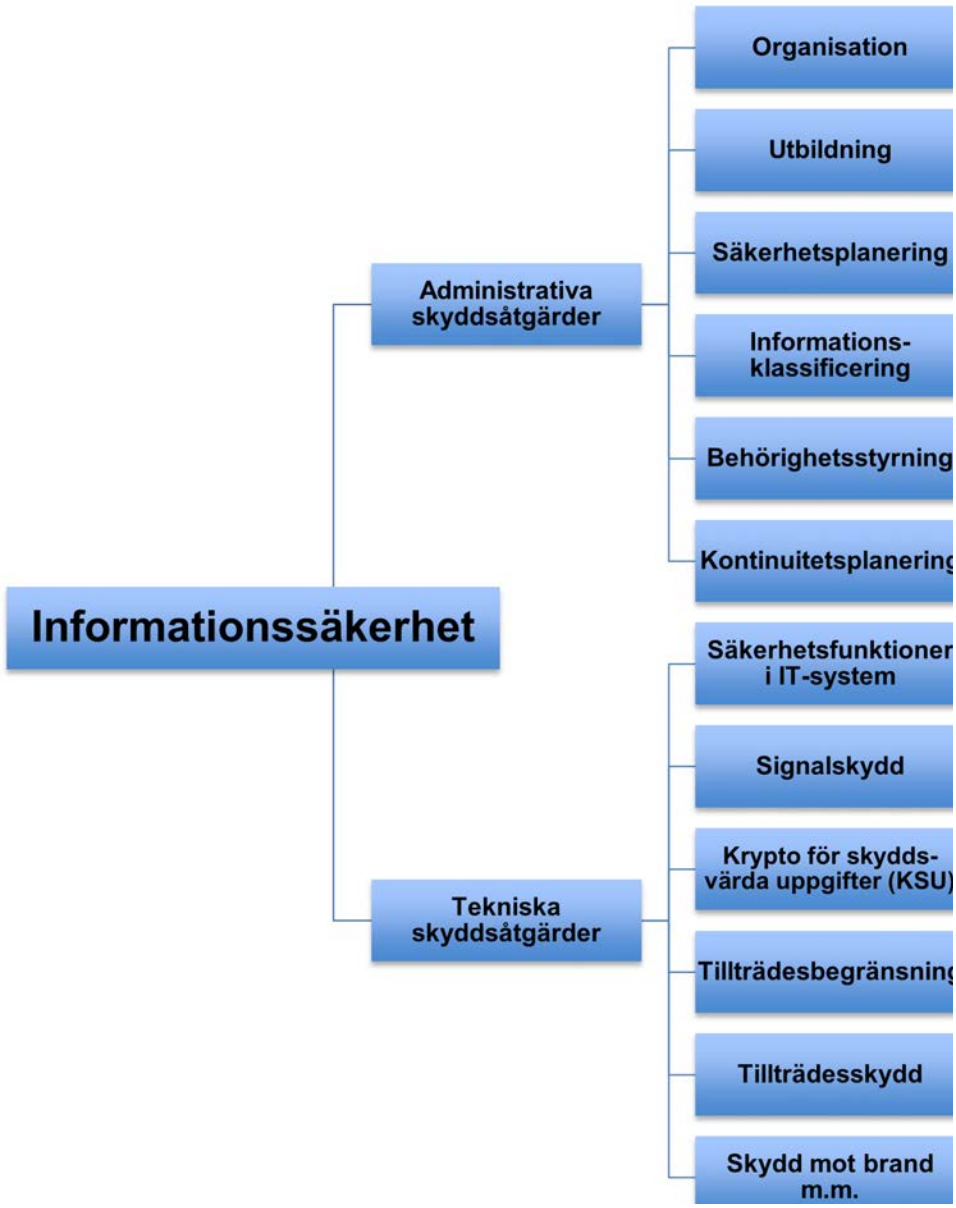


Bild 1:2 - Schematisk bild av hur informationssäkerheten kan uppnås. Andra skyddsåtgärder, än de som anges i bilden, kan förekomma.

2 Ledning av informationssäkerhet i Försvarsmakten

Arbete med informationssäkerhet i Försvarsmakten styrs internt genom regler och bestämmelser, där de grundläggande kraven på administrativa och tekniska skyddsåtgärder anges i föreskrifter, instruktioner och reglementen. Skydd av Försvarsmaktens informationstillgångar uppnås främst av att organisationsenheterna uppfyller sådana krav. Vissa krav på skyddsåtgärder är absoluta medan andra skyddsåtgärder behöver anpassas mot lokala förhållanden, t.ex. genom säkerhetsplanering där säkerhetsanalys ingår.

2.1 Försvarsmaktens informationssäkerhetspolicy

Försvarsmaktens informationssäkerhetspolicy som är baserad på de svenska standarderna SS-ISO/IEC 27001 och SS-ISO/IEC 27002 har beslutats av Överbefälhavaren. Policyn återges både på svenska och på engelska i [referens 10] respektive [referens 12]. Policyn återges i bilaga 4. Av standarderna framgår att det av en informationssäkerhetspolicy bl.a. bör framgå:

- ledningens viljedeklaration,
- fastläggande av att säkerheten är viktig i verksamheten och informationssäkerhetens betydelse för verksamheten anges,
- en definition av begreppet informationssäkerhet,
- motiv för varför och vilken säkerhet som behövs i organisationen (t.ex. risker och omvärldens krav eller förväntningar),
- övergripande mål,
- ansvarsfördelning inom organisationen med en betoning på det personliga ansvaret,
- sanktioner vid åsidosättande av policyn,
- incidenthantering,
- vem som är dokumentansvarig för policyn, hur den ska revideras och följas upp, och
- en plan för policyns förverkligande.

En informationssäkerhetspolicy innehåller inte bindande rättsregler som bestämmer enskildas och myndigheters handlande. Stöd för vilket skydd som ska finnas ska sökas i regler och bestämmelser samt andra styrande dokument. Bilaga 1 innehåller en förteckning över vissa författningar som rör informationssäkerhet i Försvarsmakten.

Sammanställning över bestämmelser och riktlinjer för säkerhetstjänsten (SAMSÄK) innehåller en förteckning över bl.a. dokument som förekommer inom den militära säkerhetstjänstens arbetsområde, inklusive dokument om informationssäkerhet. Sammanställningen utges årligen av säkerhetskontoret vid MUST.

> *Det övergripande målet med Försvarsmaktens informationssäkerhet är att säkerställa ett tillräckligt skydd för myndighetens informationstillgångar såväl inom som utom landet, så att rätt information är tillgänglig för rätt person i rätt tid på ett spårbart sätt.*
>
> Försvarsmaktens informationssäkerhetspolicy

Det övergripande målet för informationssäkerhet anger vad informationssäkerheten syftar till. Det är med tanke på Försvarsmaktens nuvarande uppgifter viktigt att påpeka att informationssäkerheten även måste upprätthållas utomlands, t.ex. vid internationella militära insatser. Ett tillräckligt skydd innebär att skyddet måste avvägas mot t.ex. lagstiftning och bedömda risker samt vad det skulle kosta att genomföra vissa åtgärder. Således ska organisationsenheterna alltid sträva efter att ha ett balanserat skydd.

Skydd i och kring ett IT-system uppnås genom att bland annat följa de föreskrifter som finns i Försvarsmaktens föreskrifter om säkerhetsskydd och Försvarsmaktens interna bestämmelser om IT-säkerhet angående godkända säkerhetsfunktioner. För att uppnå ett tillräckligt skydd i och kring ett IT-system krävs dessutom att ytterligare skyddsåtgärder identifieras, bl.a. genom verksamhets-, regelverks- och säkerhetsanalys (kapitel 14).

I informationssäkerheten som rör hemliga uppgifter ingår även att se till att tele- och datakommunikation samt andra kommunikationsvägar håller ur säkerhetssynpunkt en tillräcklig hög nivå.[5]

> *Information är en av Försvarsmaktens viktigaste tillgångar och utgör en förutsättning för att kunna bedriva verksamheten. Våra informationstillgångar måste därför behandlas och skyddas på ett tillfredsställande sätt mot de risker som förekommer. Lagar och förordningar utgör grunden för Försvarsmakten i detta arbete, dessutom ska ingångna överenskommelser och avtal följas.*
>
> Försvarsmaktens informationssäkerhetspolicy

5 Sidan 75, Säkerhetsskydd prop. 1995/96:129.

Att konstatera om en handling innehåller någon uppgift som omfattas av OSL, och därmed inte ska lämnas ut om allmänheten begär att få ta del av den, är inte tillräckligt för skyddet av uppgifterna i handlingen. Skyddet mot att uppgifter som omfattas av sekretess inte ska röjas för obehöriga behöver vara mer omfattande än att kunna ge ett nekande svar om någon vill ta del av uppgifterna enligt bestämmelserna i TF.

Risker identifieras genom att genomföra en säkerhetsanalys.[6] Risker kan även vara identifierade i den militära säkerhetstjänstens säkerhetshotbedömningar. I säkerhetsskyddslagen och säkerhetsskyddsförordningen finns bl.a. grundläggande föreskrifter om hur information som rör rikets säkerhet ska skyddas. Rättsliga krav sätter de yttre ramarna för hur informationstillgångar får hanteras i Försvarsmakten. Försvarsmakten är en statlig förvaltningsmyndighet och styrs i likhet med andra myndigheter av ett system av normer som sätter gränserna för verksamheten och som fördelar uppgifter och ansvar inom staten (bild 2:1). Skyddsåtgärderna får således inte utformas så att dessa strider mot rättsliga krav i t.ex. TF eller arkivlagen.

I detta sammanhang bör det poängteras att organisationsenheter inom Försvarsmakten inte ingår avtal sinsemellan. Istället ingår de överenskommelser mellan varandra. Samma förfaringssätt gäller mellan myndigheter.

6 1 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

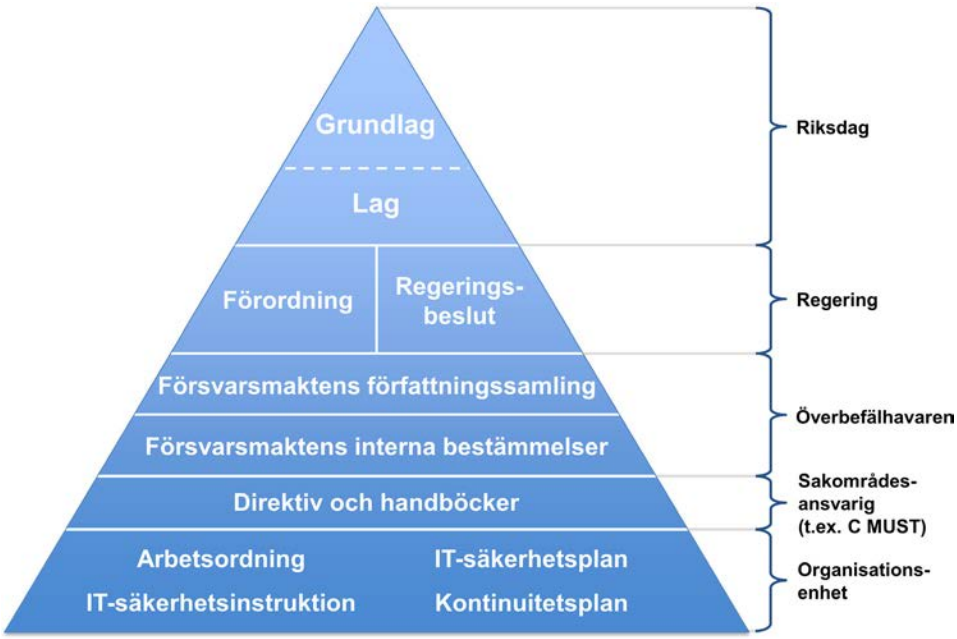


Bild 2:1 - Schematisk beskrivning av den hierarki av normer som reglerar Försvarsmaktens verksamhet med exempel på dokument med tillhörande ansvarsfördelning.

> *Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.*
>
> Försvarsmaktens informationssäkerhetspolicy

Anledningen till att både manuell och automatiserad behandling beskrivs är att informationssäkerheten inte avgränsas till att bara omfatta information på papper eller digital information i IT-system. I fråga om digital information i IT-system används även begreppet elektronisk handling. Med begreppet form avses t.ex. talad eller skriven information, men det kan också vara information (upptagningar) som enbart kan uppfattas med tekniskt hjälpmedel, t.ex. ett IT-system, eller att informationen framgår av ett föremål. Med begreppet miljö avses t.ex. ett elektroniskt kommunikationsnät, men kan också avse en fysisk brevlåda för distribution av post.

> *Informationssäkerheten omfattar Försvarsmaktens informationstillgångar utan undantag.*
>
> Försvarsmaktens informationssäkerhetspolicy

Flertalet uppgifter som förekommer i myndighetens verksamhets totala informationsmängd är uppgifter som inte omfattas av sekretess enligt OSL (benämns *Ej sekretess* i bild 2:2). En viss delmängd av de totala informationstillgångarna omfattas dock av en eller flera bestämmelser i OSL (benämns Sekretess i bild 2:2). En särtyp av de uppgifter som omfattas av sekretess är uppgifter som rör rikets säkerhet (benämns *Hemliga* i bild 2:2). I Försvarsmaktens internationella samarbeten finns uppgifter som ska skyddas som om uppgifterna rör rikets säkerhet (benämns *Utrikesklassificerade* i bild 2:2). Uppgifter som omfattas av sekretess enligt OSL men som inte är hemliga eller utrikesklassificerade förekommer också i Försvarsmakten (benämns *Sekretessklassificerade* i bild 2:2). Att informationssäkerheten i Försvarsmakten omfattar samtliga informationstillgångar innebär inte att skyddet ska vara lika för alla typer av informationstillgångar. Skyddet ska vara anpassat till informationstillgångens betydelse.

Försvarsmakten har en modell för informationsklassificering med avseende på sekretess.[7] Någon generell modell för att klassificera informationstillgångar med avseende på tillgänglighet och riktighet saknas i Försvarsmakten. Sådana modeller kan dock tillämpas inom verksamheter i Försvarsmakten.

Bild 2:2 - Försvarsmaktens informationstillgångar indelade med avseende på sekretess. Färgerna avser endast att förstärka skillnaderna och har ingen egen mening.

Informationssäkerhetspolicyn omfattar alla informationstillgångar. Även informationstillgångarna i mycket säkerhetskänslig verksamhet, t.ex. försvarsunderrättelseverksamhet, omfattas av regler och bestämmelser om informationssäkerhet även om sådan verksamhet kan vara särskilt reglerad och få personer har insyn i verksamheten.

7 Avsnitt 1.2 i H Säk Sekrbed Del A.

Med informationssäkerhet avses i Försvarsmakten:

- *att informationen finns tillgänglig när den behövs,*
- *att informationen är och förblir riktig,*
- *att informationen endast är tillgänglig för dem som är behöriga att ta del av och använda den, samt*
- *att hanteringen av informationen är spårbar.*

Försvarsmaktens definition på informationssäkerhet innebär alltså ett vidare begrepp än det som anges i säkerhetsskyddslagen.

Försvarsmaktens informationssäkerhetspolicy

Försvarsmaktens informationstillgångar ska skyddas oavsett om de omfattas av någon form av sekretess eller inte. Detta innebär att Försvarsmakten har en vidare syn på informationssäkerhet än vad som anges i säkerhetsskyddslagstiftningen. Säkerhetsskyddslagstiftningen tar enbart sikte på hemliga uppgifter.

Första punkten (tillgänglighet) innebär att informationen ska kunna utnyttjas i förväntad utsträckning och inom önskad tid.

Andra punkten (riktighet) innebär att informationens värde (t.ex. siffror) eller innebörd (t.ex. ord) över tiden ska överensstämma med det som informationen är avsedd att avspegla.[8]

Tredje punkten (sekretess) innebär att endast de som är behöriga ska få ta del av informationen. Det är inte bara hemliga uppgifter som ska skyddas, utan även andra uppgifter som omfattas av sekretess enligt OSL ska skyddas. OSL tillämplighet gäller således oavsett lagrum. Även sådan information som inte omfattas av sekretess ska skyddas. Detta innebär att information i såväl allmänna handlingar som andra handlingar ska skyddas.

Fjärde punkten (spårbarhet) innebär att det ska vara möjligt att i efterhand härleda hur informationen har hanterats, t.ex. vem som har läst en viss uppgift och när läsningen ägde rum. Detta inskränker naturligtvis inte den grundlagsskyddade meddelarfriheten. Normalt får myndigheten inte efterforska vem som har utnyttjat sin meddelarfrihet. Spårbarheten kan sägas omsluta de övriga informationssäkerhetsaspekterna (bild 2:3).

8 Definitioner på riktighet, tillgänglighet och spårbarhet framgår av SIS HB 550 Terminologi för informationssäkerhet, utgåva 3, 2007.

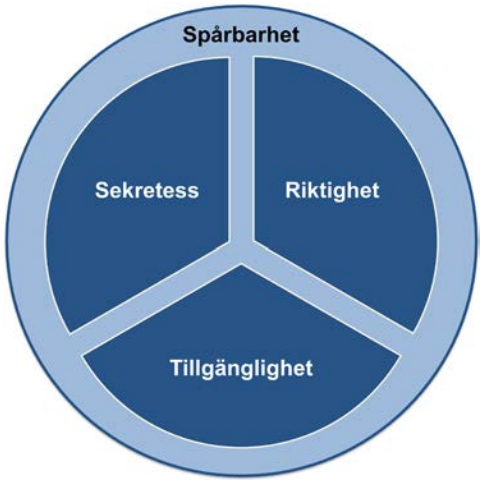


Bild 2:3 - Förhållandet mellan begreppen sekretess, riktighet, tillgänglighet samt spårbarhet.

Informationssäkerhet är en integrerad del av Försvarsmaktens verksamhet. Alla som i någon utsträckning hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är samtidigt ett ansvar för chefer på alla nivåer inom Försvarsmakten att aktivt verka för att alla inser informationssäkerhetens betydelse och att en positiv attityd till säkerhetsarbetet genomsyrar all verksamhet. Försvarsmaktens informationssäkerhetsarbete leds och samordnas av militära underrättelse- och säkerhetstjänsten i Högkvarteret. Var och en i Försvarsmakten ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgångar.

Försvarsmaktens informationssäkerhetspolicy

Det är envars ansvar att delta i säkerhetsarbetet inom sitt arbetsområde. Med alla avses civil och militär personal. Med militär personal avses yrkesofficerare, reservofficerare, anställda gruppbefäl, soldater och sjömän samt officersaspiranter, rekryter, totalförsvarspliktig personal, krigsfrivillig personal, hemvärnsmän, frivillig personal, tjänstepliktig personal och personal i Försvarsmaktens internationella militära insatser.[9] Även andra, t.ex. uppdragstagare, som deltar i Försvarsmaktens verksamhet måste ges förutsättningar att kunna skydda Försvarsmaktens informationstillgångar. Dessa kan dock inte bli föremål för myndighetens arbetsrättsliga åtgärder.

9 2 kap. 1-2 §§ förordningen med bestämmelser för Försvarsmaktens personal.

Vissa befattningar har ansvar och arbetsuppgifter för att upprätthålla informationssäkerheten, t.ex. chef för organisationsenhet, chef för kontingent i en internationell militär insats, produktägare för ett IT-system, säkerhetschef, IT-säkerhetschef och signalskyddschef.

Chefer på alla nivåer ska verka för att en positiv attityd till säkerhetsarbetet finns i verksamheten. Detta kan ske t.ex. genom att uppmuntra till utbildning och att föregå med gott exempel i förhållande till säkerhetsarbetet.

Med hänsyn till att chefen för MUST är Försvarsmaktens informationssäkerhetschef leds och samordnas myndighetens informationssäkerhetsarbete vid MUST.[10] Inom MUST är det säkerhetskontoret som handlägger frågor som rör informationssäkerhet.

Informationssäkerhetspolicyn belyser att alla måste hjälpa till vad gäller säkerhetsrapportering för att den ska fungera på ett effektivt sätt. Försvarsmaktens personal har en skyldighet att rapportera säkerhetshotande verksamhet.[11] Rapportering av incidenter är en förutsättning för att främst kunna åtgärda brister lokalt. Att rapporteringen vidarebefordras till central nivå är nödvändigt för att dra lärdomar och för att förbättra informationssäkerheten. Med hänsyn till omfattningen av informationstillgångar i IT-system och att sårbarheter kan få omfattande konsekvenser finns det ett krav på omedelbar rapportering för händelser som kan påverka säkerheten i och kring Försvarsmaktens IT-system.[12]

> *Informationssäkerhetspolicyn förverkligas genom att vi följer de mål, handlingsplaner och åtgärder som beskrivs i Försvarsmaktens regelverk.*
>
> Försvarsmaktens informationssäkerhetspolicy

Med Försvarsmaktens regelverk avses regler (föreskrifter [FFS och FIB] och allmänna råd [FAR]), bestämmelser (instruktioner och reglementen), handböcker och manualer samt styrande dokument.

> *Varje organisationsenhet är bunden av denna policy, vilket medför att det inte finns något utrymme att besluta om lokala policies som avviker från denna informationssäkerhetspolicy.*
>
> Försvarsmaktens informationssäkerhetspolicy

10 11 kap. 5 § Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).
11 4 kap. 2 § Försvarsmaktens föreskrifter för Försvarsmaktens personal.
12 2 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

En organisationsenhet inom Försvarsmakten får inte meddela undantag från Försvarsmaktens informationssäkerhetspolicy. Däremot kan en organisationsenhet ha en lokal informationssäkerhetspolicy som svarar mot enhetens lokala förhållanden, under förutsättning att den policyn inte strider mot den myndighetsgemensamma informationssäkerhetspolicyn. Den lokala policyn bör heller inte vara en upprepning av Försvarsmaktens informationssäkerhetspolicy.

Lokala förhållanden kan t.ex. vara detaljerade beskrivningar av vilka utbildningar som olika personalkategorier måste ha genomgått med godkänt resultat för att få hantera olika informationstillgångar.

> *Den som använder Försvarsmaktens informationstillgångar på ett sätt som strider mot denna informationssäkerhetspolicy kan bli föremål för åtgärder från myndighetens sida.*
>
> Försvarsmaktens informationssäkerhetspolicy

Åtgärder från myndighetens sida kan t.ex. vara chefssamtal eller att behörighet till viss information tas bort.

> *Militära underrättelse- och säkerhetstjänsten i Högkvarteret ansvarar för att informationssäkerhetspolicyn årligen granskas och vid behov revideras.*
>
> Försvarsmaktens informationssäkerhetspolicy

Försvarsmaktens informationssäkerhetspolicy är tänkt att gälla över lång tid. För att policyn ska kunna hållas aktuell ska den dock granskas varje år och vid behov revideras. Inom MUST är det säkerhetskontoret som ansvarar för granskningen.

> *Denna informationssäkerhetspolicy är fastställd av överbefälhavaren den 5 april 2005 och ska börja tillämpas den 1 maj 2005.*
>
> Försvarsmaktens informationssäkerhetspolicy

Överbefälhavaren har genom beslutet att fastställa informationssäkerhetspolicyn givit uttryck för myndighetsledningens viljeinriktning vad gäller Försvarsmaktens informationssäkerhet.

2.2 Organisation

För att säkerställa att säkerhetsrelaterade frågor i och kring ett IT-system beaktas, är det nödvändigt att det finns en fungerande organisation som kan ta hand om de säkerhetsrelaterade frågor som kan uppkomma. Detta gäller från det att beslut tas om utveckling av ett IT-system till dess att det driftsätts eller avvecklas, d.v.s. under IT-systemets livscykel. Erfarenheter har visat att i de fall då IT-säkerhet inte beaktas tidigt, föreligger stora risker för kostnadsökning och försening.

I Försvarsmaktens organisation är IT-säkerhetsarbetet normalt uppdelat på följande aktörer:

- Central nivå – Produktägare (PÄ) och produktansvarig samt säkerhetskontoret vid MUST.
- Lokal nivå – Systemägare (SÄ), IT-säkerhetschef, biträdande IT-säkerhetschef och i förekommande fall garnisonschef.
- Driftorganisation – Driftägare (DÄ) och driftansvarig (DA).

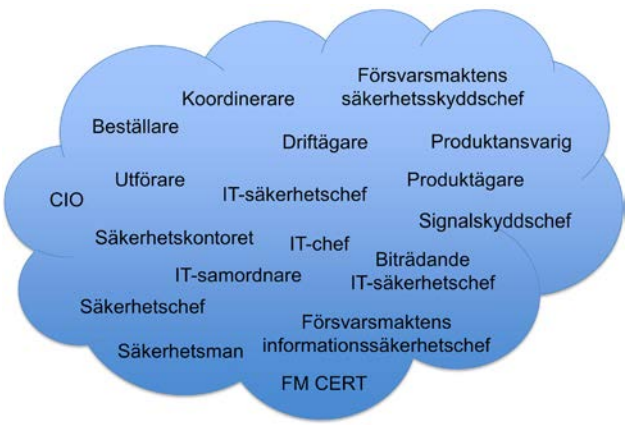


Bild 2:4 - Några av alla de aktörer som förekommer i Försvarsmaktens IT-säkerhetsarbete.

I arbete med informationssäkerhet, inklusive IT-säkerhet, förekommer naturligt samarbete med andra delar av den militära säkerhetstjänsten, t.ex. signalskyddstjänsten. För att uppnå en god säkerhet i och kring ett IT-system är det av stor vikt att de berörda aktörerna (bild 2:4) är medvetna om sina roller, avgränsningarna för den egna rollen och de andra rollerna samt beröringspunkterna dem emellan.

2.2.1 Chefen för MUST

Chefen för militära underrättelse- och säkerhetstjänsten är Försvarsmaktens säkerhetsskyddschef och utövar kontroll över säkerhetsskyddet i enlighet med 6 § säkerhetsskyddsförordningen (1996:633) samt är tillika Försvarsmaktens informationssäkerhetschef.

Chefen för militära underrättelse- och säkerhetstjänsten ska leda och samordna totalförsvarets signalskyddstjänst, inklusive arbetet med säkra kryptologiska funktioner som är avsedda att skydda skyddsvärd information, och föreslå föreskrifter som ska beslutas av överbefälhavaren i frågor om signalskyddstjänsten inom totalförsvaret i enlighet med vad som föreskrivs i 33 § förordningen (2007:1266) med instruktion för Försvarsmakten, samt förhandla internationella signalskyddsöverenskommelser.

I uppgiften ingår att stödja produktionschefen vid anskaffning av säkra kryptografiska funktioner samt med yttrande avseende IT-säkerhet.

11 kap. 5 § Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO)

Av 6 § säkerhetsskyddsförordningen framgår att det vid en myndighet ska, om det inte är uppenbart obehövligt, finnas en säkerhetsskyddschef som utövar kontroll över säkerhetsskyddet. Chefen för MUST är Försvarsmaktens säkerhetsskyddschef.

Chefen för MUST ska planera, leda, genomföra och följa upp militär säkerhetstjänst.[13] Chefen för MUST ska leda och samordna utvecklingen av militär säkerhetstjänst inom Försvarsmakten inom ramen för Försvarsmaktens utvecklingsplan och överbefälhavarens inriktningsbeslut.[14] Detta innebär att chefen utfärdar instruktioner, direktiv och handböcker inom den militära säkerhetstjänstens område.

Chefen för MUST är även Försvarsmaktens informationssäkerhetschef. På samma sätt som det inte finns mer än en säkerhetsskyddschef i myndigheten finns det inget behov av att organisationsenheterna utser informationssäkerhetschefer. Försvarsmaktens chefer och medarbetare ska i stället gemensamt bidra till ett funktionellt och förutseende informationssäkerhetsarbete. På lokal nivå representeras den militära säkerhetstjänsten av säkerhetschefer, IT-säkerhetschefer samt signalskyddschefer.

Vad gäller signalskyddstjänsten hänvisas till H TST Grunder.

13 11 kap. 1 § Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO)
14 11 kap. 6 § Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).

Chefen för militära underrättelse- och säkerhetstjänsten i Högkvarteret ska leda sådan kontrollverksamhet som rör säkerheten i och kring IT-system som inte är avsedda för behandling av hemliga uppgifter. Militära underrättelse- och säkerhetstjänsten samt operativa enheten i Högkvarteret får genomföra kontroller av säkerheten i och kring sådana IT-system vid organisationsenheterna.

13 kap. 2 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Föreskriften innebär bl.a. att chefen för MUST kan fatta beslut om hur sådan kontrollverksamhet ska genomföras. Med i och kring förstås att det inte enbart är IT-systemet som ska kontrolleras utan även sådana förhållanden kring IT-systemet som kan påverka dess säkerhet. Som exempel kan nämnas tillträdesskydd som skalskydd och inpasseringskontroll för lokaler och andra utrymmen för IT-system.

2.2.2 Produktägare

Till produktägare får utses den chef som har ansvaret för den verksamhet som ett IT-system huvudsakligen skall stödja. CIO, eller den han eller hon bestämmer, utser produktägare. Ett beslut att utse någon till produktägare skall dokumenteras.

4 § Försvarsmaktens interna bestämmelser om IT-verksamhet

I dessa bestämmelser avses med produktägare: den som är utsedd att vara produktägare enligt 4 § Försvarsmaktens interna bestämmelser (FIB 2007:5) om IT-verksamhet.

1 kap. 6 § 13 Försvarsmaktens interna bestämmelser om IT-säkerhet

En produktägare i Försvarsmakten har på flera sätt en central roll i fråga om IT-säkerhet:

- En produktägare ska i Försvarsmakten leda, samordna och avdela resurser för IT-verksamheten under ett IT-systems livscykel.[15]
- Produktägaren, eller den han eller hon bestämmer, ska besluta vem som är behörig att hantera källkoder.[16]

15 7 § Försvarsmaktens interna bestämmelser om IT-verksamhet.
16 10 § Försvarsmaktens interna bestämmelser om IT-verksamhet

- Produktägaren ska tillsammans med driftägaren se till att det finns aktuella ritningar som beskriver de IT-system och elektroniska kommunikationsnät som var och en svarar för (avsnitt 17.3).[17]
- En produktägare är den som beslutar om ett IT-system, som är anslutet till ett elektroniskt kommunikationsnät som har tillhandahållits av Försvarsmakten, ska få anslutas till ett elektroniskt kommunikationsnät som inte har tillhandahållits av Försvarsmakten (avsnitt 17.2).[18]
- En produktägare ska se till att säkerhetslogg i ett IT-system kan analyseras och att loggen har erforderlig detaljeringsgrad (avsnitt 18.4.3).[19]
- En produktägare ska besluta om central ackreditering av ett IT-system (avsnitt 19.3). Innan ett sådant beslut fattas ska produktägaren se till att säkerheten i och kring IT-systemet har granskats och se till att det särskilt beaktas hur IT-systemet är avsett att samverka med andra IT-system (avsnitt 19.1).[20]
- En produktägare ska se till att en systemägare förses med erforderligt underlag och erforderliga resurser så att systemägaren kan fatta beslut om lokal ackreditering (avsnitt 19.4).[21]
- En produktägare bör ta fram grunden för den överenskommelse som ska gälla mellan systemägaren och driftägaren för ett IT-system. En sådan överenskommelse kallas normalt SLA (engelska: Service Level Agreement). Överenskommelsen bör innehålla riktlinjer för hur en god IT-säkerhet kan uppnås. Exempelvis bör gränsdragningar avseende ansvar och uppgifter finnas i överenskommelsen, t.ex. hur IT-säkerhetskontroller får genomföras, från ett verksamhets- och driftsperspektiv. Överenskommelsen bör även omfatta riktlinjer för hur aktörerna bör stödja varandra i IT-säkerhetsfrågor för att om möjligt merutnyttja kompetens och resurser (utan att göra avkall på respektive rolls integritet). Sådana aktörer kan t.ex. vara en organisationsenhets IT-säkerhetschef, företrädare för driftägaren samt garnisonschef.

Endast en chef som har ansvaret för den verksamhet som ett IT-system huvudsakligen ska stödja kan av CIO utses till produktägare.[22] Många IT-system i Försvarsmakten levereras som en gemensam IT-tjänst. För sådana IT-system är det naturligt att CIO är produktägare. I Försvarsmakten finns även IT-system som endast stöder avgränsade verksamheter. Rollen produktägare är inte genom någon författning begränsad till centrala verksamhetsutövare Till produktägare utses normalt centrala verksamhetsutövare. Normalfallet är att produktägare finns vid Högkvarteret.

17 12 § Försvarsmaktens interna bestämmelser om IT-verksamhet.
18 5 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
19 8 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
20 12 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
21 12 kap. 5 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
22 4 § Försvarsmaktens interna bestämmelser om IT-verksamhet.

För materiel finns rollen *ägarföreträdare*. Produktionschefen är ägarföreträdare för Försvarsmaktens materiel.[23] Chef som har ansvaret för den verksamhet som ett IT-system huvudsakligen ska stödja kan vara någon annan än produktionschefen. För materiel, som är eller som innehåller IT-system, kan därför rollerna produktägare och ägarföreträdare innehas av olika chefer.

2.2.3 Chef för organisationsenhet

Organisationsenheterna utgörs av Högkvarteret samt av förband, skolor och centrum, vilka är angivna som organisationsenheter i förordningen med instruktion för Försvarsmakten.[24] Krigsförband och hemvärnsförband ingår i organisationsenheterna.

En chef för en organisationsenhet ansvarar från ett säkerhetsperspektiv för bl.a. följande.

- Att den som genomför utbildning i säkerhetstjänst har tillräcklig kunskap och erfarenhet.[25]
- Se till att den som får ta del av hemliga uppgifter har upplysts om räckvidden och innebörden av sekretessen och att ett sekretessbevis upprättas. Får delegeras.[26]
- Får lämna medgivande till kopiering eller utdrag ur en handling som är placerad i informationssäkerhetsklass HEMLIG/TOP SECRET. Får delegeras.[27]
- Se till att en företrädare för en utländsk myndighet eller en mellanfolklig organisation uppvisar ett intyg om säkerhetsklarering innan företrädaren tar del av hemliga eller utrikesklassificerade uppgifter. Får delegeras.[28]
- Ska lämna ett godkännande om vilka lokaler och områden som är godkända ur säkerhetssynpunkt (skydd mot avlyssning) för muntlig delgivning av hemliga och utrikesklassificerade uppgifter som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre. Får delegeras.[29]
- Besluta var och hur hemliga och utrikesklassificerade handlingar ska förvaras.[30]
- Får besluta om samförvaring och gemensam användning av hemliga och utrikesklassificerade handlingar. Får delegeras.[31]

23 9 kap. 3 § andra stycket i Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).
24 2 kap. 4 § andra stycket och bilaga 2 i Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).
25 Avsnitt 3.2 i Instruktion avseende kunskapskrav säkerhetstjänst [referens 41].
26 2 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
27 2 kap. 9 § Försvarsmaktens föreskrifter om säkerhetsskydd.
28 2 kap. 2 a § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
29 2 kap. 3 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
30 2 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
31 2 kap. 7-8 §§ Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

- Får besluta om medförande av en hemlig eller utrikesklassificerad handling som har placerats i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre. Får delegeras.[32]
- Fastställa riktlinjer för IT-säkerheten inom organisationsenheten (skriftlig IT-säkerhetsplan).[33]
- Fatta beslut om att IT-system, som inte är avsedda för att användas för överföring av uppgifter via ett elektroniskt kommunikationsnät som har tillhandahållits av Försvarsmakten, får användas för överföring av uppgifter till ett annat tillgängligt elektroniskt kommunikationsnät.[34]
- Se till att användare har genomgått erforderlig utbildning i IT-säkerhet med godkänt resultat och kan hantera IT-systemet på ett säkert sätt, innan de tilldelas behörighet att utnyttja det.[35]
- Ska besluta vem som är behörig att använda eller ta del av uppgifter i ett IT-system. Får delegeras.[36]
- Se till att användare av ett IT-system informeras om att säkerhetsloggning sker.[37]
- Ska genomföra kontroller av säkerheten i och kring sådana IT-system inom enheten som inte är avsedda för behandling av hemliga eller utrikesklassificerade uppgifter.[38]
- Ska vara systemägare för ett IT-system i det fall han eller hon ansvarar för en del av IT-systemet som ska användas i den egna verksamheten (avsnitt 2.2.4).[39]

En krigsförbandschef eller en hemvärnschef har inte rätt att fatta de beslut som beskrivits ovan om inte beslutsrätten har delegerats. En förutsättning för sådana fall är att beslutsrätten får delegeras.

Det är naturligt att organisationsenhetens säkerhetschef och IT-säkerhetschef lämnar stöd till en chef för en organisationsenhet. Det är lämpligt att arbetsuppgifter som rör säkerhetsområdet delegeras till säkerhetschef och IT-säkerhetschef.

32 2 kap. 10 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
33 1 kap. 10 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
34 5 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
35 6 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
36 7 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
37 8 kap. 5 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
38 13 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
39 1 kap. 6 § 14 Försvarsmaktens interna bestämmelser om IT-säkerhet.

2.2.4 Systemägare

I dessa bestämmelser avses med systemägare: den chef för en organisationsenhet som ansvarar för den del av ett IT-system som ska användas i den egna verksamheten.

1 kap. 6 § 14 Försvarsmaktens interna bestämmelser om IT-säkerhet

Endast en chef för en organisationsenhet kan vara systemägare. För ett IT-system som används av flera systemägare ansvarar respektive systemägare för den del av IT-systemet som enbart är till för systemägarens verksamhet.

IT-verksamheten i Försvarsmakten har effektiviserats bl.a. genom konsolidering av programvaror och hårdvara. IT-system är i stor utsträckning centraliserade och används av personal vid samtliga organisationsenheter. Denna utveckling har medfört ett behov av ändrad syn på rollen som systemägare. I de fall en chef för en organisationsenhet inte ansvarar för den delen av ett IT-system som ska användas i organisationsenhetens verksamhet är rollen systemägare inte tillämplig för det aktuella IT-systemet (exempel 2:1). När det inte finns hårdvara lokalt, t.ex. lokala klienter, och IT-systemet används på en lokalt ackrediterad plattform, t.ex. FM AP, är rollen *system*ägare inte relevant. Så länge som det lokalt finns hårdvara som ingår i IT-systemet är rollen systemägare relevant. Det bör av auktorisationsbeslut för ett IT-system framgå när rollen systemägare inte är relevant för IT-systemet.

Exempel 2:1

Vid I 19 finns, liksom vid övriga organisationsenheter, IT-systemet Charon som ger tillgång till Internet. Charon är en IT-tjänst som levereras centralt till användare i Försvarsmakten. CIO är produktägare till Charon. Chefen för I 19 ansvarar inte för de delar av Charon som ska användas i organisationsenhetens verksamhet. Chefen för I 19 är således inte systemägare till Charon.

En systemägare ska för ett IT-system som ska användas i den egna verksamheten besluta om lokal ackreditering (avsnitt 19.4) om systemägaren ansvarar för IT-systemet i den egna verksamheten.[40] En systemägare ska ha inhämtat samråd från garnisonschefen innan han eller hon beslutar om lokal ackreditering av ett IT-system som ska användas gemensamt inom garnisonen.[41]

40 12 kap. 5 § första stycket Försvarsmaktens interna bestämmelser om IT-säkerhet.
41 12 kap. 5 § tredje stycket Försvarsmaktens interna bestämmelser om IT-säkerhet.

Systemägaren, eller den han eller hon bestämmer, ska se till att säkerhetsloggar analyseras (avsnitt 18.4.3).[42] I det fall rollen systemägare inte ska finnas för ett IT-system är det produktägaren som bör ta över systemägarens uppgifter, t.ex. att se till att säkerhetsloggar analyseras.

2.2.5 Säkerhetschef

Vid varje organisationsenhet ska det finnas en säkerhetschef.

Uppgifter som anges i säkerhetsskyddsförordningen och i Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd och som får anses ankomma på säkerhetsskyddschefen ankommer, såvitt avser säkerhetsskyddet vid en organisationsenhet, på säkerhetschefen vid organisationsenheten.

1 kap. 4 § andra och tredje styckena Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Några uppgifter om informationssäkerhet som direkt kan anses ankomma på säkerhetschefen vid en organisationsenhet förekommer inte i säkerhetsskyddsförordningen eller Försvarsmaktens föreskrifter om säkerhetsskydd. I H SÄK Grunder beskrivs däremot vilket ansvar som säkerhetschefen har med stöd av den lokala säkerhetsorganisationen och vilken utbildning som en säkerhetschef ska ha gått.

2.2.6 IT-säkerhetschef

Vid varje organisationsenhet ska det finnas en IT-säkerhetschef som leder och samordnar IT-säkerhetsarbetet direkt under säkerhetschefen.

1 kap. 11 § första stycket Försvarsmaktens interna bestämmelser om IT-säkerhet

Föreskriften lägger inget hinder för att en IT-säkerhetschef kan ha andra arbetsuppgifter inom en organisationsenhet. Erfarenheter visar dock att IT-säkerheten kan bli lidande om IT-säkerhetschefen även har andra arbetsuppgifter. Därför bör IT-säkerhetschefen inte ha andra arbetsuppgifter än de som tillkommer denne som IT-säkerhetschef. En IT-säkerhetschef bör således inte vara IT-chef. Detta för att undvika intressekonflikter som kan uppstå om IT-säkerhetschefen granskar de beslut och åtgärder som han eller hon har fattat i rollen som IT-chef.

42 8 kap. 4 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

Med hänsyn till de alltmer komplicerade frågor som rör IT-säkerhet är det befogat att varje organisationsenhet ska ha en IT-säkerhetschef. IT-säkerhetschefen är underställd organisationsenhetens säkerhetschef. Anledningen är bl.a. att säkerhetschefen är direkt underställd chefen för organisationsenheten såvitt avser säkerhetsärenden.

Inom ramen för IT-säkerhetschefens ledning och samordning av IT-säkerhetsarbetet vid organisationsenheten kan följande uppgifter ankomma på IT-säkerhetschefen.

- Leda framtagning av riktlinjer för IT-säkerhet (IT-säkerhetsplan).
- Vara rådgivare i IT-säkerhetsfrågor inom säkerhetsskyddsområdet.
- Vara rådgivare i IT-säkerhetsfrågor utom säkerhetsskyddsområdet.
- Samordna IT-säkerhetsarbetet; vid behov i samverkan med IT-chefen och driftägaren.
- Stödja genomförandet av analyser som t.ex. säkerhetsanalyser.
- Kontrollera att författningar som rör IT-säkerhet samt att IT-säkerhetsplan och eventuella övriga riktlinjer för IT-säkerheten följs.
- Leda kontroller av säkerhetsloggar; i förekommande fall bör det ske i samverkan med driftägaren.
- Leda utbildning av IT-säkerhet samt ansvara för förmedling av information om IT-säkerhet.
- Lämna stöd vid anskaffning av IT-system, för att se till att kraven avseende säkerhetsskydd samt övrig säkerhet tillgodoses.
- Lämna stöd vid framtagning av planer som rör vilka åtgärder som ska vidtas vid avbrott eller störningar i ett IT-systems funktion (kontinuitetsplanering).
- Leda, genomföra och protokollföra interna kontroller vad avser IT-säkerhet; i förekommande fall bör det ske i samförstånd med driftägaren.
- Vara ett stöd för systemägaren inför dennes beställning av IT-säkerhetsfunktionalitet från driftansvarig inom ramen för SLA.
- Samverka med driftägaren i ärenden som rör hantering av IT-säkerhetsrelaterade incidenter.

Det bör även ankomma på IT-säkerhetschefen att ge säkerhetsmannen den utbildning som krävs för att säkerhetsmannen ska kunna fullgöra sina uppgifter. Vidare är det lämpligt att IT-säkerhetschefen går de utbildningar som i övrigt ges inom säkerhetsområdet vid organisationsenheten. Med hänsyn till den ständiga förändring som sker inom IT-säkerhetsområdet är det också viktigt att en IT-säkerhetschef kontinuerligt ges möjlighet till erforderlig kompetensutveckling.

En befattning som IT-säkerhetschef får inte tillsättas utan att vederbörande har genomgått erforderlig utbildning i IT-säkerhet med godkänt resultat eller förvärvat motsvarande kunskap på annat sätt.

6 kap. 2 § Försvarsmaktens interna bestämmelser om IT-säkerhet

En IT-säkerhetschefs uppgifter och IT-säkerhetens betydelse för informationssäkerheten motiverar kravet på utbildning. Den utbildning som ges inom Försvarsmakten är Försvarsmaktens IT-säkerhetschefsutbildning som genomförs av Försvarsmaktens underrättelse- och säkerhetscentrum (FMUndSäkC).

Utbildningen bör ge kunskaper för att kunna arbeta som IT-säkerhetschef inom en organisationsenhet och oberoende av om befattningen är placerad inom eller utom landet. Utbildningen måste kunna skapa förutsättningar för den tilltänkte IT-säkerhetschefen att kunna leda, planera, utbilda inom och kontrollera IT-säkerheten inom egen organisationsenhet. Vidare bör den tilltänkte IT-säkerhetschefen efter utbildningen ha goda kunskaper i det regelverk som styr Försvarsmaktens IT-säkerhet. IT-säkerhetschefen bör också ha sådana tekniska kunskaper så att han eller hon kan tillgodogöra sig informationsteknikens möjligheter och begränsningar.

Med hänsyn till de uppgifter som ankommer på en biträdande IT-säkerhetschef och en IT-säkerhetsansvarig är det lämpligt att även de genomgår samma utbildning som en IT-säkerhetschef.

Föreskriften medger även att adekvat IT-säkerhetskunskap kan ha inhämtats på annat sätt än genom utbildning. Sådan kunskap kan ha förvärvats t.ex. genom lång tjänstgöringstid som IT-säkerhetschef eller motsvarande.

Enbart kommersiella personcertifieringar[43] är inte tillräckligt för att uppfylla föreskriften då de bl.a. inte tar upp det regelverk som styr Försvarsmaktens IT-säkerhet. Personcertifieringar och kurser i IT-säkerhet vid t.ex. Totalförsvarets forskningsinstitut och Försvarshögskolan kan däremot tillföra kunskap som stärker Försvarsmaktens IT-säkerhetsarbete, särskilt med tanke på den snabba utvecklingen inom området.

43 T.ex. Information Security Management Professional (ISMP), Certified Information Systems Security Professional (CISSP) eller Certified Information Security Manager (CISM).

2.2.7 Biträdande IT-säkerhetschef

Om någon del av en organisationsenhet är belägen på en annan plats än den där enheten huvudsakligen är lokaliserad ska chefen för organisationsenheten överväga om det på den platsen behövs en biträdande IT-säkerhetschef.

1 kap. 11 § andra stycket Försvarsmaktens interna bestämmelser om IT-säkerhet

Med hänsyn till att det idag finns organisationsenheter som är belägna på annan plats än den där enheten huvudsakligen är belägen ska chefen för organisationsenheten överväga om det på den platsen behövs en biträdande IT-säkerhetschef (exempel 2:2).

Exempel 2:2

I Blekinge flygflottilj (F 17) ingår specialflygenheten fpl 100/102 (Malmen), vilken är belägen i Linköping. Föreskriften innebär att chefen för F 17 ska överväga om det behövs en biträdande IT-säkerhetschef vid Malmen i Linköping.

De uppgifter som ankommer på en IT-säkerhetschef bör även ankomma på den biträdande IT-säkerhetschefen, således måste en biträdande IT-säkerhetschef ha samma utbildning som en IT-säkerhetschef. Vidare bör den biträdande IT-säkerhetschefen samverka med IT-säkerhetschefen.

2.2.8 IT-säkerhetsansvarig

Vid utveckling och anskaffning av ett IT-system ska det, om det inte är uppenbart obehövligt, finnas en IT-säkerhetsansvarig som leder och samordnar IT-säkerhetsarbetet.

1 kap. 11 § tredje stycket Försvarsmaktens interna bestämmelser om IT-säkerhet

För att säkerställa att IT-säkerheten beaktas från det att beslut tas om att utveckla ett IT-system till dess att det tas i drift, är det i regel nödvändigt att en IT-säkerhetsansvarig utses inom t.ex. det projekt som leder framtagningen av IT-systemet. Erfarenheter har visat att det i de fall då IT-säkerheten inte beaktas tidigt, finns stora risker för kostnadsökning och försening.

Utvecklingens eller anskaffningens omfattning får avgöra om det ska finnas en IT-säkerhetsansvarig. En IT-säkerhetsansvarig får vara en annan person än IT-säkerhetschefen.

De uppgifter som kan ankomma på en IT-säkerhetsansvarig i frågor som rör utveckling eller anskaffning av ett IT-system kan följande nämnas.

- Leda framtagning av riktlinjer för IT-säkerhet.
- Vara rådgivare i IT-säkerhetsfrågor.
- Samordna IT-säkerhetsarbetet och vid behov i samverkan med IT-chef och driftägaren.
- Stödja genomförandet av analyser som t.ex. säkerhetsanalyser.
- Stödja produktansvarig i framtagning av auktorisationsunderlag och ackrediteringsunderlag avseende IT-säkerhetsfrågor.
- Kontrollera att författningar som rör IT-säkerhet och att riktlinjer för IT-säkerheten följs.
- Leda kontroller av säkerhetsloggar; i förekommande fall bör det ske i samverkan med driftägaren.
- Leda utbildning av IT-säkerhet samt ansvara för förmedling av information om IT-säkerhet.
- Lämna stöd vid anskaffning av IT-system, så att kraven avseende säkerhetsskydd samt övrig säkerhet tillgodoses.
- Leda, genomföra och protokollföra interna kontroller vad avser IT-säkerhet.
- Stödja vid framtagning av planer som rör vilka åtgärder som ska vidtas vid avbrott eller störningar i ett IT-systems funktion (kontinuitetsplanering).

Om den IT-säkerhetsansvarige är en annan person än IT-säkerhetschefen, bör samverkan ske med honom eller henne.

En IT-säkerhetsansvarigs utbildning vara samma som utbildningen för en IT-säkerhetschef. En IT-säkerhetsansvarig kan dock behöva specifika kunskaper om utveckling och anskaffning av IT-system, t.ex. säkerhet i IT-arkitektur, säker kodning och testmetoder. En bra bakgrund för en IT-säkerhetsansvarig är att tidigare ha arbetat i befattning som IT-säkerhetschef.

2.2.9 Säkerhetsman

En säkerhetsman kan bl.a. ha till uppgift att stödja upprätthållandet av IT-säkerheten inom egen enhet. Syftet med en sådan säkerhetsman är att denne kan verifiera att regelverk och planer följs. En säkerhetsman bör även vara ett nära stöd till verksamhetsansvariga chefer inom IT-säkerhetsområdet. Till skillnad från en IT-säkerhetschef

har en säkerhetsman även andra uppgifter vid sidan av att han eller hon är säkerhetsman.

Utöver de uppgifter som framgår av H SÄK Grunder kan uppgifter på en säkerhetsman i fråga om IT-säkerhet vara följande.

- Under IT-säkerhetschefen ansvara för det dagliga IT-säkerhetsarbetet, t.ex. daglig kontroll av säkerhetsloggar.
- Medverka vid genomförandet av IT-säkerhetsanalyser.
- Ge råd i IT-säkerhetsfrågor.
- Stödja verksamheten vid framtagning av underlag för ackreditering av IT-system.
- Stödja verksamheten vid framtagning av planer för vilka åtgärder som ska vidtas vid avbrott eller störningar (kontinuitetsplanering).
- Medverka vid anskaffning av IT-system, för att se till att krav på säkerhet tillgodoses.

2.2.10 Garnisonschef

Rollen garnisonschef förekommer inte längre i FM ArbO. Det är produktionschefen som ska leda och samordna verksamheten mellan organisationsenheter (garnisonssamordning) inom samma kommun eller liknande samordning mellan organisationsenheter i olika kommuner.[44] Med garnisonssamordning avses bl.a. säkerhetstjänst.[45] När garnisonschef förekommer i Försvarsmaktens interna bestämmelser om IT-säkerhet får bestämmelserna tolkas utifrån garnisonssamordningen.

> *Varje garnisonschef eller den han bestämmer ska genomföra och dokumentera hot-, risk- och sårbarhetsanalyser i fråga om ett IT-system som ska användas gemensamt inom garnisonen och utifrån analyserna vidta lämpliga skyddsåtgärder.*
>
> 4 kap. 2 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Föreskriften gäller både IT-system som är avsedda för behandling av hemliga uppgifter och övriga IT-system. Stöd för hur analysarbetet kan genomföras framgår av avsnitt 14.4. Analysarbetet ska dokumenteras i en säkerhetsmålsättning.[46]

44 9 kap. 6 § Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).
45 Bilaga 2 till Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).
46 4 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

Innan en systemägare beslutar om lokal ackreditering av ett IT-system som ska användas gemensamt inom en garnison, ska han ha inhämtat samråd från garnisonschefen.

12 kap. 5 § tredje stycket Försvarsmaktens interna bestämmelser om IT-säkerhet

På orter med fler än en organisationsenhet lyder en chef för en organisationsenhet under garnisonschefen avseende bl.a. säkerhetstjänst.[47] Med hänsyn till detta lydnadsförhållande ska en systemägare innan han eller hon får fatta beslut om lokal ackreditering för ett IT-system som ska användas gemensamt inom en garnison, ha inhämtat samråd från garnisonschefen. Om garnisonschefen inte samråder får inte systemägaren fatta beslut om lokal ackreditering.

En garnisonschef får inom ramen för sitt samordningsansvar genomföra kontroller av säkerheten i och kring IT-system som inte är avsedda för behandling av hemliga uppgifter.

13 kap. 3 § andra stycket Försvarsmaktens interna bestämmelser om IT-säkerhet

Med hemliga uppgifter avses även utrikesklassificerade uppgifter. Det är lämpligt att genomföra en sådan kontroll som framgår av föreskriften en gång varje år. Vidare bör garnisonschefen inom ramen för sitt samordningsansvar även få genomföra kontroller av säkerheten i och kring IT-system som är avsedda för behandling av hemliga eller utrikesklassificerade uppgifter. Garnisonschefen bör även utse en av de lokala IT-säkerhetscheferna för att samordna garnisonens IT-säkerhetsverksamhet avseende kontroller.

2.2.11 Driftägare

I dessa bestämmelser avses med driftägare: den chef för en organisationsenhet som ansvarar för driften av IT-system.

2 § 5 Försvarsmaktens interna bestämmelser om IT-verksamhet

IT-säkerhetskontroller som genomförs inom ramen för driftägarens ansvar (överenskommet i SLA) bör samordnas med berörd organisationsenhets IT-säkerhetschef. IT-säkerhetskontroller av garnisonsgemensamma system samordnas genom garnisson-

47 18 kap. 5 § Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).

samordning.[48] Vidare bör driftägaren leda kontroller av IT-systemens driftjournaler. En driftägare har även en roll i arbetet med utarbeta, vidmakthålla, testa och genomföra en kontinuitetsplan för ett IT-system (avsnitt 14.6).

2.3 Försvarsmaktens IT-styrmodell

I Försvarsmakten finns en IT-styrmodell som reglerar hur IS/IT och informationsinfrastruktur ska styras [referens 37]. IT-styrmodellen beskriver övergripande vilka roller som fattar vilka typer av beslut, beställer, levererar och följer upp leveranser av de IT-tjänster som ger verksamheten i Försvarsmakten det IT-stöd som efterfrågas. Nedan beskrivs rollerna i IT-styrmodellen.

Beställare	Centrala verksamhetsutövare och sakområdesansvariga som ställer verksamhetskrav på en IT-tjänst, beslutar om, beställer och ansvarar för att denna finansieras. En beställare är ansvarig för verksamhet eller sakområde enligt Försvarsmaktens arbetsordning och ansvarar för att den nytta verksamheten får av IT-tjänsten uppväger kostnaderna. Eftersom beställaren ansvarar för verksamheten ska beställaren också ta ett centralt ansvar för säkerheten och risker som är förknippad med IT-tjänsten.
IT-samordnare	Stödjer beställaren med att omsätta verksamhetens behov till beställningsbara krav på IT-tjänster, omsätta regler, riktlinjer och förändringar för sakområde IS/IT till tillämpbara handlingsregler för den egna verksamheten samt budgetera, följa upp kostnaderna och genomföra kostnads- och nyttoanalys.
Koordinerare	Sammanställer och koordinerar kravställningen på IT-tjänster. Koordineraren ansvarar också för att inrikta, beställa, kontrollera och följa upp produktionen av IT-tjänster. Koordinatorn är leveransansvarig mot beställaren. Finns på strategisk (CIO) och operativ nivå (produktionsledningen i Högkvarteret).
Utförare	De som producerar och tillhandahåller IT-tjänster enligt lagda beställningar.
Produktionsansvarig	Bryter ned de samlade uppdragen från koordinatorn till detaljerade interna uppdrag och externa avtal till externa leverantörer och interna utförare.
Intern utförare	Organisationsenhet som erhåller uppdrag att leverera hel eller del av IT-tjänst.
Extern leverantör	Andra myndigheter, företag och organisationer som via avtal förbinder sig att leverera hel eller del av IT-tjänst.
Nyttjare	De som använder IT-tjänsterna i verksamheten.

48 9 kap. 6 § Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).

En aktör inom IT-området kan agera i flera roller, t.ex. vid de organisationsenheter där nyttjarna också har en utförarroll.

Koordineraren ska samordna kravställning med olika regelverk, t.ex. IT-säkerhet, och komplettera med tekniska krav. Enligt IT-styrmodellen kan C MUST aktivt delta i kravställning, lösningsframtagning, leverans samt i granskning och kontroll för att säkerställa rätt funktionalitet och hög kvalitet.

Produktägare (avsnitt 2.2.2) motsvaras i IT-styrmodellen normalt av rollen *beställare*. Det kan även förekomma att andra chefer än centrala verksamhetsutövare är produktägare.

I IT-styrmodellen definieras roller som inte finns i Försvarsmaktens interna bestämmelser om IT-verksamhet eller Försvarsmaktens interna bestämmelser om IT-säkerhet. I IT-styrmodellen beskrivs IT-system på ett sätt som kan uppfattas inskränka definitionen i Försvarsmaktens föreskrifter om säkerhetsskydd, Försvarsmaktens interna bestämmelser om IT-säkerhet och Försvarsmaktens interna bestämmelser om IT-verksamhet. Betydelsen av begreppet IT-system är i fråga om IT-säkerhet bredare än vad som följer av IT-styrmodellen. Ett arbete kommer att initieras för att se över författningarna.

IT-styrmodellen får inte användas på ett sätt som skulle medföra att föreskrifter, i t.ex. Försvarsmaktens interna bestämmelser om IT-verksamhet eller Försvarsmaktens interna bestämmelser om IT-säkerhet, inte följs (se bild 2:1 för en schematisk beskrivning av den hierarki av normer som reglerar Försvarsmaktens verksamhet).

2.4 Materielanskaffning

Försvarets materielverk anskaffar försvarsmateriel på uppdrag av Försvarsmakten. Ett samordningsavtal [referens 40] mellan Försvarsmakten och Försvarets materielverk har slutits i syfte att övergripande samordna relationer och rutiner mellan myndigheterna.

Vid anskaffning av materiel ska Försvarsmakten ange direkta krav på informationssäkerhet, inklusive IT-säkerhet.[49] Sådana krav kan t.ex. anges i målsättningar och kravdokument. Försvarets materielverk följer enligt samordningsavtalet de föreskrifter och handböcker inom informationssäkerhetsområdet, inklusive IT-säkerhet, som Försvarsmakten fastställer.[49]

Se även avsnitt 14.1.1 om säkerhetsmålsättning vid materielanskaffning och avsnitt 21 om avveckling.

49 § A 9.5 Samordningsavtal mellan Försvarsmakten och Försvarets materielverk [referens 40].

2.5 Upphandling av konsulttjänster eller IT-system

När upphandling av konsulttjänster eller IT-system ska göras, ska beställaren före upphandlingen pröva om upphandlingen helt eller delvis ska skyddas med hänsyn till rikets säkerhet.[50] Berör upphandlingen arbete med hemliga uppgifter eller materiel eller anskaffning av IT-system som är avsedda för behandling av hemliga uppgifter ska den skyddas genom ett säkerhetsskyddsavtal.[51]

Analys ska alltid göras inför upphandlingen för att de säkerhetsskyddskrav som behövs ska kunna specificeras i förfrågningsunderlaget i anslutning till det som ska upphandlas.[52] [53] Skyddet måste vara en naturlig del av anbudet eller upphandlingen och vägas mot de uppgifter som ska skyddas.

En säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA) syftar, vid en upphandling, till att skapa ett säkerhetsskydd för hemliga uppgifter. Riktlinjer i arbetet med säkerhetsskydd av upphandling finns i Handbok Säkerhetsskyddad upphandling med säkerhetsskyddsavtal (Handbok SUA). Bestämmelser om sådan upphandling finns i lagen om upphandling på försvars- och säkerhetsområdet.

För upphandling av konsulttjänster för arbete med utrikesklassificerade eller sekretessklassificerade uppgifter finns föreskrifter om *skyddad upphandling* i 2 kap. 9-11 §§ respektive 3 kap. 18-19 §§ Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

2.6 Ledning av informationssäkerhet under höjd beredskap

Krav på skyddsåtgärder som rör informationssäkerhet (t.ex. i Försvarsmaktens föreskrifter om säkerhetsskydd och Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel) är för närvarande utformade med utgångspunkt från att kraven ska gälla även under skärpt och högsta beredskap.

50 8 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd.
51 8 § säkerhetsskyddslagen.
52 1 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd.
53 7 kap. 7-8 §§ Försvarsmaktens föreskrifter om säkerhetsskydd.

3 Ledning av informationssäkerhet vid andra myndigheter

Myndigheten för samhällsskydd och beredskap har föreskrivit att myndigheter under regeringen ska tillämpa ett ledningssystem för informationssäkerhet.[54] Föreskrifterna gäller inte Regeringskansliet, kommittéväsendet och Försvarsmakten.[55] [56] En myndighet som omfattas av föreskrifterna ska arbeta med informationssäkerhet i former som följer standarderna SS-ISO/IEC 27001:2006 och SS-ISO/IEC 27002:2005.[57] Föreskrifterna gäller inte om det i någon annan författning, t.ex. i säkerhetsskyddslagstiftningen, finns bestämmelser om statliga myndigheters arbete med informationssäkerhet.[58] Föreskrifter om informationssäkerhet i säkerhetsskyddslagstiftningen gäller endast för hemliga uppgifter.

Om en myndighet har ett ledningssystem för informationssäkerhet som följer ovan nämnda standarder bör ledningssystemet även omfatta informationssäkerhet för hemliga uppgifter. I ett s.k. uttalande om tillämplighet enligt standarderna är det i sådana fall lämpligt att ange hur åtgärdsmål och säkerhetskrav för skydd av hemliga uppgifter är kopplade till säkerhetsskyddslagstiftningens krav.

Säkerhetsskyddet vid en myndighet ska utformas med hänsyn till verksamhetens art, omfattning och övriga omständigheter.[59] Då olika myndigheter har skilda behov av säkerhetsskydd kan utformningen av skyddsåtgärderna därför skilja sig åt mellan olika myndigheter.

54 4 § Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.
55 3 och 34 §§ förordningen om krisberedskap och höjd beredskap.
56 2 § Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.
57 6 § Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.
58 3 § Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.
59 5 § första stycket säkerhetsskyddslagen.

Myndigheterna skall meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) i fråga om säkerhetsskyddet inom sina verksamhetsområden, om det inte är uppenbart obehövligt. Om det behövs skall myndigheterna innan dess samråda med den myndighet som enligt 43 och 44 §§ meddelar föreskrifter för myndighetens område.

Myndigheternas föreskrifter får avvika från föreskrifterna enligt 43 och 44 §§ endast om detta har medgivits av den myndighet som har meddelat dessa föreskrifter.

45 § säkerhetsskyddsförordningen

Med ytterligare föreskrifter avses de interna föreskrifter om säkerhetsskydd som behöver finnas vid en myndighet. En myndighets interna föreskrifter om säkerhetsskydd får endast avvika från föreskrifterna i Försvarsmaktens föreskrifter om säkerhetsskydd om detta har medgivits av Försvarsmakten.[60] Ett ärende om Försvarsmaktens medgivande bereds genom säkerhetskontoret vid MUST.

Innan en myndighet som omfattas av Försvarsmaktens föreskrifter om säkerhetsskydd meddelar sådana interna föreskrifter ska myndigheten, om det behövs, samråda med Försvarsmakten.[61] Med hänsyn till informationssäkerhetsområdets komplexitet bör samråd med säkerhetskontoret vid MUST alltid ske.

Statliga myndigheter, kommuner och landsting för vilka Rikspolisstyrelsen (Säkerhetspolisen) i fråga om säkerhetsskydd har föreskriftsrätt, ska följa Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd. För Regeringskansliet, kommittéväsendet, riksdagen och myndigheter under riksdagen gäller andra föreskrifter om säkerhetsskydd.

60 45 § andra stycket säkerhetsskyddsförordningen.
61 45 § säkerhetsskyddsförordningen.

4 Ledning av informationssäkerhet i internationella samarbeten

Olika stater och mellanfolkliga organisationer har olika regelverk för informationssäkerhet. I ett internationellt samarbete, där uppgifter som omfattas av sekretess enligt de olika ländernas regelverk ska hanteras, behöver regelverk för informationssäkerhet uppmärksammas.

Inför ett internationellt samarbete där det kan förutsättas att uppgifter som omfattas av sekretess enligt OSL kommer att lämnas till en annan stat eller mellanfolklig organisation måste förutsättningarna för skyddet av uppgifterna klarläggas. För ett utbyte av hemliga eller utrikesklassificerade uppgifter bör det finnas ett säkerhetsskyddsavtal med den andra staten eller organisationen.[62] Ytterligare detaljerade regler kan behöva anges i andra typer av avtal (t.ex. Technical Arrangement) för det specifika samarbetet.[63]

Grunden för ledningen av informationssäkerhet är vems regi samarbetet bedrivs i. Om en svensk myndighet svarar för samarbetet är grundprincipen att det är det regelverk som den myndigheten har att följa som även ska gälla i samarbetet, t.ex. i fråga om eventuell utländsk personals hantering av gemensamma handlingar i en svensk myndighets lokaler. På motsvarande sätt ska personal från en svensk myndighet som tjänstgör i en internationell stab följa det regelverk som gäller där för de handlingar som hanteras i samarbetet. Om handlingar däremot lämnas över till företrädare till det andra landet så gäller det landets säkerhetsbestämmelser.

För att en svensk myndighet ska få lämna uppgifter som omfattas av sekretess enligt OSL till en annan stat eller mellanfolklig organisation krävs att vissa villkor är uppfyllda (se avsnitt 7.7). För svenska handlingar som inte avses lämnas till en utländsk myndighet eller mellanfolklig organisation och som hanteras i det internationella samarbetet av svensk personal gäller det svenska regelverket för skydd av handlingarna.

> *Om det i ett avtal för visst internationellt samarbete förekommer bestämmelser om säkerhetsskydd som avviker från föreskrifterna i denna författning skall bestämmelserna i avtalet ha företräde.*
>
> 9 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

62 Säkerhetsskyddsavtal med andra stater och mellanfolkliga organisationer publiceras normalt på regeringens webbplats under Sveriges internationella överenskommelser (SÖ).

63 Se även Försvarsmaktens interna bestämmelser om rätten att förhandla, ingå, ändra och säga upp internationella överenskommelser m.m.

I vissa fall förekommer det att skyddsbestämmelser tas in i internationella avtal eller i säkerhetsskyddsavtal mellan två eller flera länder. Det är viktigt att Sverige lever upp till de bestämmelser som har avtalats med andra stater och mellanfolkliga organisationer och därför ska skyddsbestämmelser i sådana avtal äga företräde framför bestämmelserna i Försvarsmaktens föreskrifter om säkerhetsskydd. Avvikelserna kan utgöras av såväl minskade som ökade krav på säkerhetsskydd för vissa uppgifter eller handlingar.

Föreskriften gäller även för skyddsbestämmelser i internationella avtal eller i säkerhetsskyddsavtal som avser skydd av utrikesklassificerade uppgifter.[64]

Om det i ett avtal för visst internationellt samarbete förekommer bestämmelser om säkerhetsskydd som avviker från bestämmelserna i denna författning ska bestämmelserna i avtalet ha företräde.

Tillämpning av sådana bestämmelser som avses i första stycket ska, om möjligt, föregås av samråd med militära underrättelse- och säkerhetstjänsten i Högkvarteret. Har sådant samråd inte skett ska militära underrättelse- och säkerhetstjänsten i Högkvarteret snarast underrättas.

9 kap. 6 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Inom MUST är det säkerhetskontoret som handlägger frågor som rör informationssäkerhet. Det är lämpligt att samråd sker med säkerhetskontoret under planeringsarbetet för ett internationellt samarbete.

Om det i verksamhet där personal har ställts till förfogande för annan stat eller mellanfolklig organisation gäller bestämmelser om skydd av uppgifter i den verksamheten, och som avviker från föreskrifterna i denna författning, ska bestämmelserna ha företräde.

1 kap. 10 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

När ansvaret för ett förband övergår från Sverige till en mellanfolklig organisation övergår även ansvaret för säkerhetsfrågorna på den organisationen. När det gäller nationella delar och nationell verksamhet kvarstår dock det nationella säkerhetsansvaret. Det kan t.ex. röra sig om personaladministration, logistikärenden till och från

64 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Sverige och säkerhetstjänst (exempelvis säkerhetsskyddet för hemliga uppgifter och handlingar som förekommer under insatsen).

För den verksamhet som bedrivs under den mellanfolkliga organisationens regi kan det meddelas bestämmelser om skydd för uppgifterna som förekommer där. Bestämmelserna för skyddet kan skilja sig från Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar. Denna paragraf tydliggör därför att sådana internationella bestämmelser då ska tillämpas även om de avviker från Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

I verksamhet där den andra staten eller mellanfolkliga organisationen inte har meddelat bestämmelser om skydd för uppgifterna som förekommer där ska Försvarsmaktens regelverk tillämpas.

För försändelser med hemliga handlingar till utlandet skall Utrikesdepartementets kurirförbindelser anlitas.

Rikspolisstyrelsen och Försvarsmakten kan för sina respektive tillsynsområden enligt 39 § besluta om undantag från första stycket.

11 § säkerhetsskyddsförordningen

Varje myndighet får i avtal med ett annat land eller mellanfolklig organisation komma överens om att distribuera hemliga handlingar på annat sätt än vad som föreskrivs i 11 § första stycket säkerhetsskyddsförordningen (1996:633).

2 kap. 25 § tredje stycket Försvarsmaktens föreskrifter om säkerhetsskydd

I vissa fall kan internationell verksamhet ställa andra krav på överföring av hemliga handlingar än vad ordinarie kurirförbindelser kan uppfylla. I dessa fall får myndigheterna och organisationsenheterna i Försvarsmakten[65] komma överens med mottagande land eller organisation på vilket sätt överföringen kan ske. I dessa fall minskar naturligtvis skyddet för handlingarna vilket bör beaktas.

65 1 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

Om det i avtal för visst internationellt samarbete förekommer bestämmelser om skydd som avviker från bestämmelserna i 1 kap. såvitt avser sekretessklassificerade handlingar och 3 kap. ska bestämmelserna i avtalet ha företräde.

3 kap. 20 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Föreskriften avser bestämmelser för skydd av sekretessklassificerade uppgifter. Något samråd med MUST behöver inte genomföras.

4.1 Europeiska unionen (EU)

Säkerhetsbestämmelser för Europeiska unionens råd gäller inom EU för att skydda EU-uppgifter som har klassificerats efter en indelning i fyra nivåer.[66] Säkerhetsbestämmelserna ska gälla för rådet och generalsekretariatet och ska iakttas av medlemsstaterna i enlighet med deras nationella lagstiftning. Bestämmelserna är alltså inte tvingande för en svensk myndighet, inte ens för EU-handlingar som förvaras vid en svensk myndighet.[67] Om en sådan handling förvaras vid en svensk myndighet och inte bedöms röra rikets säkerhet saknas nationella föreskrifter om hur uppgifterna ska skyddas.

I Försvarsmakten ska en EU-handling som har försetts med en märkning enligt säkerhetsbestämmelsernas indelning i fyra nivåer och som inte rör rikets säkerhet klassificeras som en *utrikesklassificerad* handling. En sådan handling ska placeras i en informationssäkerhetsklass som motsvarar den nivå som handlingen enligt säkerhetsbestämmelserna har placerats i.[68]

Se även beskrivningen av utrikessekretessen och placering av utrikesklassificerade uppgifter i informationssäkerhetsklass i H Säk Sekrbed A.

66 2011/292/EU: Rådets beslut av den 31 mars 2011 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter.

67 Artikel 4.3 i EU-fördraget beskriver en lojalitetsprincip inom den Europeiska unionen. Det går därför att diskutera om inte denna princip åtminstone indirekt medför en förpliktelse för medlemsstaterna att skydda EU-uppgifter på ett sätt som motsvarar rådets säkerhetsbestämmelser.

68 1 kap. 3 § punkterna 2 och 3 samt 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

4.2 North Atlantic Treaty Organization (Nato)

Sverige har ingått ett säkerhetsskyddsavtal med Nato.[69] I avtalets artikel 4 anges att separata administrativa bestämmelser ska utarbetas mellan Sverige och Nato. Ett avtal (Administrative Arrangement for the Handling and Protection of NATO Classified Information Provided to Sweden) med sådana bestämmelser har undertecknats den 14 juni 2012 [referens 44]. På motsvarande sätt som för EU-handlingar som inte rör rikets säkerhet saknas nationella föreskrifter om hur uppgifter från Nato ska skyddas.

I Försvarsmakten ska en handling från Nato som har försetts med en märkning som motsvarar en informationssäkerhetsklass och som inte rör rikets säkerhet klassificeras som en *utrikesklassificerad* handling. En sådan handling ska placeras i en informationssäkerhetsklass som motsvarar den nivå som handlingen enligt säkerhetsbestämmelserna har placerats i.[70]

Se även beskrivningen av utrikessekretessen och placering av utrikesklassificerade uppgifter i informationssäkerhetsklass i H Säk Sekrbed A.

Nato har ett omfattande regelverk för informationssäkerhet. En svensk myndighet omfattas inte av detta regelverk, inte ens i fråga om hantering av handlingar som har sitt ursprung i Nato. Personal från en svensk myndighet kan genom tjänstgöring på en Nato-stab eller motsvarande komma i kontakt med Nato-handlingar. För skydd av sådana handlingar där personalen tjänstgör gäller Natos regelverk.

Se avsnitt 9.11.7 om förvaring av Nato-handlingar.

Se avsnitt 10.4 om användning av svenska signalskyddssystem för att skydda Nato-uppgifter.

69 Avtalet som är daterad den 6 september 1994 finns inte publicerat på regeringens webbplats under Sveriges internationella överenskommelser (SÖ).

70 1 kap. 3 § punkterna 2 och 3 samt 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretesskvalificerade uppgifter och handlingar.

5 Skydd mot brand, vatten och skadlig klimat- och miljöpåverkan

Försvarsmaktens regelverk som rör informationssäkerhet innehåller inga direkta krav vad gäller att skydd av en myndighets informationstillgångar mot skador till följd av brand, översvämning eller skadlig klimat- och miljöpåverkan. Ett verksamhetsbehov av tillgänglighet och vilka skyddsåtgärder som därmed behöver vidtas för skydd mot sådana skador bör undersökas i en säkerhetsanalys. Verksamhetens krav på tillgänglighet i ett IT-system analyseras i en verksamhetsanalys (avsnitt 14.2.2). Krav på skyddsåtgärder i och kring ett IT-system för att upprätthålla tillgänglighet är exempel på *tillkommande säkerhetskrav* för ett IT-system (avsnitt 13.3).

Boken *Skydd mot brand* utgiven av Myndigheten för samhällsskydd och beredskap kan användas som en introduktion till området förebyggande brandskydd (bilaga 1 innehåller hänvisning till boken). Det finns flera regelverk som rör brandskydd och det finns flera myndigheter och branschorganisationer som har uppgifter inom området.

En myndighet ska skydda ett arkiv mot förstörelse, skada, tillgrepp och obehörig åtkomst.[71] Utifrån arkivlagen är det inte tillräckligt att en arkivlokal för hemliga handlingar endast utformas för att uppfylla en skyddsnivå enligt 2 kap. 13-17 §§ Försvarsmaktens föreskrifter om säkerhetsskydd. Riksarkivet har meddelat bestämmelser om arkivlokaler.[72] Riksarkivets föreskrifter gäller utöver Försvarsmaktens regelverk i fråga om arkivlokaler. För att ge arkivlokaler ett tillräckligt skydd mot bl.a. brand är det nödvändigt att även Riksarkivets föreskrifter uppmärksammas vid etablering och drift av arkivlokaler. Riksarkivet har gett ut broschyren *Skydda ditt arkiv – Bygg rätt!*

På grund av IT och telekommunikationers betydelse för Försvarsmaktens verksamhet måste utrymmen för IT- och telekommunikation (t.ex. datorcentraler) särskilt uppmärksammas vad gäller skydd mot brand, vatten och skadlig klimat- och miljöpåverkan. Se även avsnitt 14.6 om kontinuitetsplanering för IT-system.

71 6 § 3 arkivlagen.
72 Riksarkivets föreskrifter och allmänna råd om arkivlokaler.

6 Informationsklassificering

Modellen för informationsklassificering i Försvarsmakten utgår från en bedömning av om en uppgift omfattas av sekretess eller inte. I OSL ges bestämmelser om när en uppgift omfattas av sekretess. Denna lag utgör grunden för bedömning av om en uppgift omfattas av sekretess eller inte och är det första steget i klassificering av information i Försvarsmakten. Uppgifter vilka omfattas av sekretess indelas i sekretesskategorierna *hemliga* (H), *kvalificerat hemliga* (KH), *utrikesklassificerade* (UK) respektive *sekretessklassificerade* (SK) uppgifter. Hemliga och utrikesklassificerade uppgifter placeras alltid i en av fyra *informationssäkerhetsklasser; HEMLIG/TOP SECRET* (H/TS), *HEMLIG/SECRET* (H/S), *HEMLIG/CONFIDENTIAL* (H/C) och *HEMLIG/ RESTRICTED* (H/R).

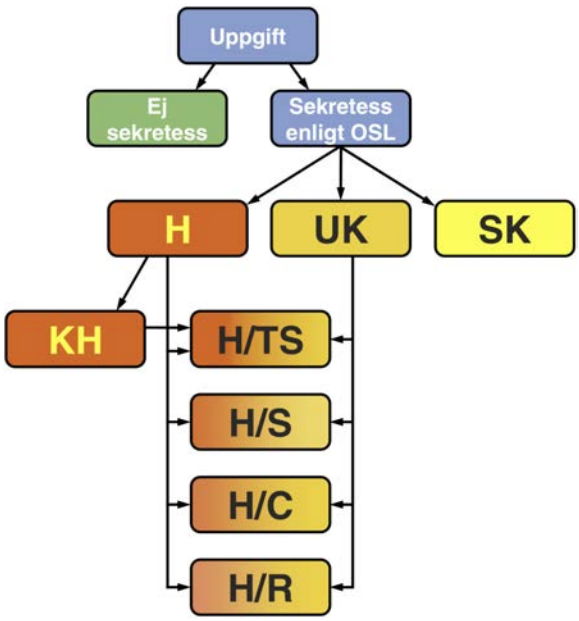


Bild 6:1 - Försvarsmaktens modell för informationsklassificering.

Vilket skydd, i form av t.ex. IT-säkerhet, signalskydd eller krypto för skyddsvärda uppgifter och tillträdesbegränsning, som ska ges en uppgift styrs av uppgiftens informationsklassificering (bild 6:2). Skyddet är starkare för hemliga uppgifter. Skyddet för hemliga och utrikesklassificerade uppgifter indelas i informationssäkerhetsklasser där en högre informationssäkerhetsklass ger ett starkare skydd (bild 6:3).

En informationsklassificering som utgår från vilket skydd som i det enskilda fallet är önskvärt, istället för att utgå från bedömning av skada eller men vid ett röjande, är en felaktig informationsklassificering. Ett exempel är om hemliga uppgifter placeras

i informationssäkerhetsklass HEMLIG/RESTRICTED istället för en högre informationssäkerhetsklass med motiveringen att det skulle underlätta hanteringen. Även det omvända att hemliga uppgifter placeras i en högre informationssäkerhetsklass för att uppgifterna ska ges ett mer omfattande skydd, även om villkoren för att placera uppgifterna i en sådan högre informationssäkerhetsklass inte är uppfyllda, är en felaktig informationsklassificering. Att felaktigt placera uppgifter i en lägre informationssäkerhetsklass medför att uppgifterna inte kommer att ges det skydd som uppgifterna behöver.

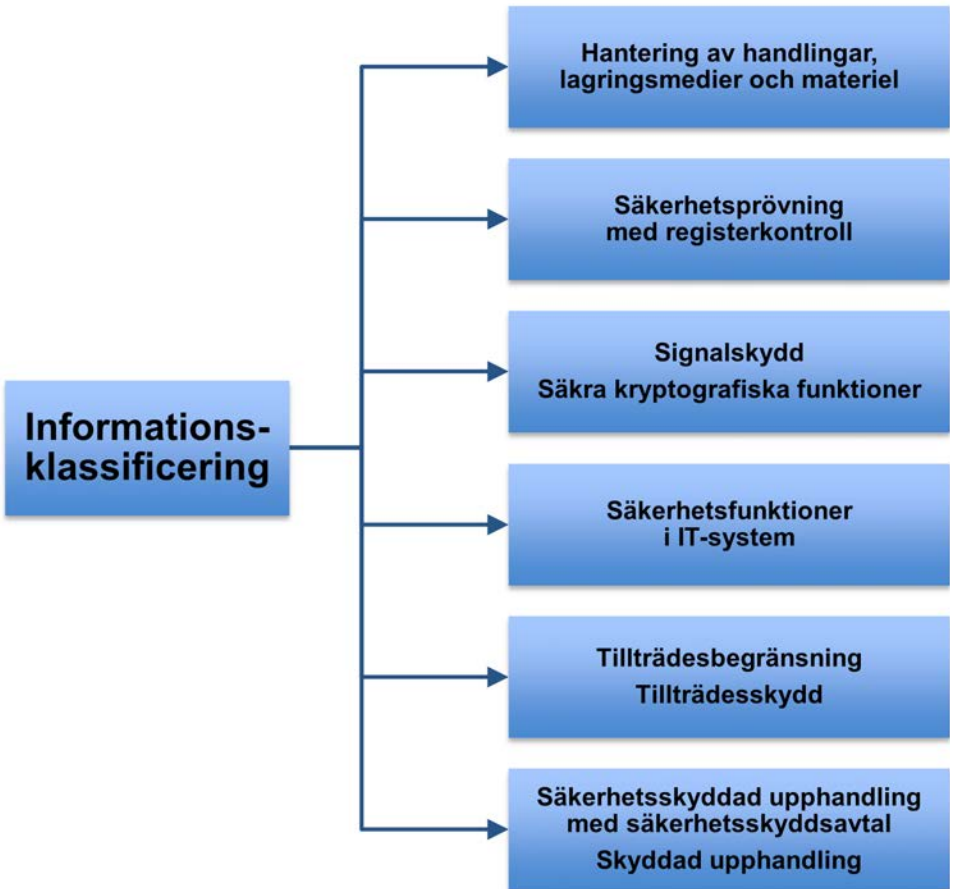


Bild 6:2 - Informationsklassificeringen styr direkt eller påverkar utformningen av olika slag av skyddsåtgärder.

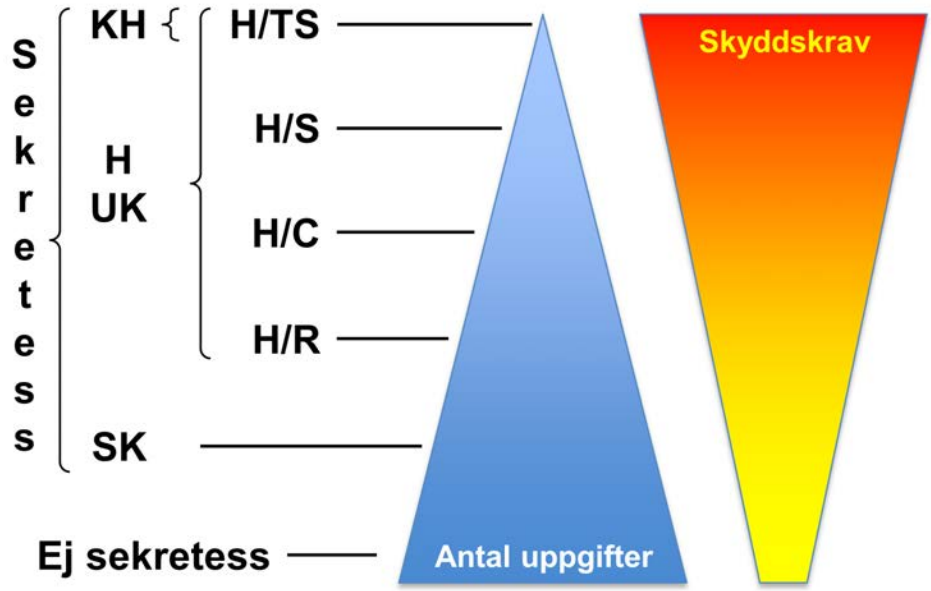


Bild 6:3 - Schematisk skiss över antal uppgifter i förhållande till de skyddskrav som gäller för uppgifterna.

6.1 Hemliga och kvalificerat hemliga uppgifter

Om en uppgift omfattas av sekretess och rör rikets säkerhet är uppgiften en *hemlig uppgift* enligt säkerhetsskyddsförordningen.[73] Om en hemlig uppgift är av synnerlig betydelse för rikets säkerhet är uppgiften *kvalificerat hemlig* (KH).[74] För uppgifter som rör rikets säkerhet ska det finnas ett skydd enligt säkerhetsskyddslagstiftningen som benämns säkerhetsskydd som främst avser skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet.[75]

Hemliga uppgifter ska enligt Försvarsmaktens föreskrifter om säkerhetsskydd placeras i informationssäkerhetsklass.[76] Det finns fyra informationssäkerhetsklasser och dessa är indelade efter vilket men som kan uppstå om uppgifterna röjs. Observera att det inte uteslutande är uppgifter som omfattas av sekretess enligt 15 kap. 2 § OSL (försvarssekretess) som kan utgöra hemliga uppgifter. Även uppgifter som omfattas av sekretess enligt 15 kap. 1 § OSL (utrikessekretess) och 18 kap. 1 § OSL (förundersökningssekretess) kan i vissa fall röra rikets säkerhet och därmed vara hemliga uppgifter.

73 4 § 1 säkerhetsskyddsförordningen.
74 1 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd.
75 6 § säkerhetsskyddslagen.
76 2 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Det skydd för en hemlig handling som föreskrivs i Försvarsmaktens föreskrifter om säkerhetsskydd och Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel gäller även för en kvalificerat hemlig handling om inget annat särskilt har angetts i författningarna.[77] För kvalificerat hemliga handlingar som är allmänna handlingar finns det en missuppfattning att sådana handlingar alltid ska sändas till Regeringskansliet. Sannolikt har uppfattningen sitt ursprung i vem som enligt 1 § OSF ska pröva frågan om utlämnande av sådana handlingar.

I svenskt språkbruk används begreppet *hemlig* för uppgifter som förknippas med någon form av konfidentialitet och då inte nödvändigtvis sekretess enligt OSL. I juridisk litteratur kan begreppet hemlig användas för uppgifter som omfattas av sekretess enligt OSL även om uppgiften inte rör rikets säkerhet. För att undvika missförstånd är det därför viktigt att försäkra sig om att de personer som använder begreppet har samma uppfattning om begreppets innebörd. Detta kan ske med ett påstående eller en kontrollfråga som innehåller ”som rör rikets säkerhet?”

Om en hemlig handling även innehåller utrikesklassificerade och sekretessklassificerade uppgifter, eller någon av de båda, benämns handlingen alltid hemlig.

6.2 Utrikesklassificerade uppgifter

Om en uppgift:

- omfattas av sekretess enligt 15 kap. 1 § OSL, s.k. utrikessekretess, men inte rör rikets säkerhet, och av
  - utländsk myndighet,
  - mellanfolklig organisation eller av
  - svensk myndighet
- har klassificerats i någon av nivåerna TOP SECRET, SECRET, CONFIDENTIAL eller RESTRICTED eller i motsvarande nivåer på andra språk,

så utgör uppgiften en *utrikesklassificerad uppgift* enligt Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.[78]

Det finns inget krav på att Sverige ska ha ingått ett säkerhetsskyddsavtal med den andra staten eller mellanfolkliga organisationen för att uppgifterna ska vara utrikesklassificerade.

77 1 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd.
78 1 kap. 3 § 2 Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Utrikesklassificerade uppgifter ska också placeras i informationssäkerhetsklass.[79] En *utrikesklassificerad handling* är en handling som innehåller utrikesklassificerad uppgift.[80] Om en utrikesklassificerad handling även innehåller sekretessklassificerade uppgifter benämns handlingen alltid utrikesklassificerad.

6.3 Sekretessklassificerade uppgifter

Övriga uppgifter vilka omfattas av sekretess, men vilka inte är hemliga eller utrikesklassificerade, benämns *sekretessklassificerade uppgifter* enligt Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.[81] Uppgifter i denna sekretesskategori ska inte placeras i informationssäkerhetsklass, eftersom uppgifterna varken är hemliga eller utrikesklassificerade. Sekretessklassificerade uppgifter ska normalt alltså inte ges samma skydd som hemliga eller utrikesklassificerade uppgifter. Sekretessklassificerade uppgifter ska däremot ges ett visst skydd vilket framgår av nämnda föreskrifter.

En *sekretessklassificerad handling* är en handling som innehåller sekretessklassificerad uppgift.[82]

6.4 Informationssäkerhetsklasser

Informationssäkerhetsklasserna är en indelning av säkerhetsskyddet i Försvarsmakten, samt i de myndigheter för vilka Försvarsmakten har föreskriftsrätt över. Då det är hemliga uppgifter som ska ges ett säkerhetsskydd ska en hemlig uppgift placeras i informationssäkerhetsklass. Även hemliga handlingar och hemlig materiel placeras i informationssäkerhetsklass då dessa innehåller hemliga uppgifter.

Informationssäkerhetsklasserna har följande beteckningar[83], förkortningar, betydelser[83] och konsekvensbeskrivningar.

79 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.
80 1 kap. 2 § 3 Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.
81 1 kap. 2 § 4 Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.
82 1 kap. 2 § 5 Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.
83 1 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Informationssäkerhetsklass	Betydelse	Konsekvensbeskrivning
HEMLIG/TOP SECRET Förkortning: H/TS	1. Hemliga uppgifter vars röjande kan medföra synnerligt men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har försetts med beteckningen TOP SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.	Förväntade konsekvenser medför en synnerlig negativ effekt. Konsekvenserna innebär synnerligen allvarliga negativa effekter av stor omfattning, under lång tid och utgör ett direkt hot mot organisationen. Konsekvenserna är inte begränsade till enstaka förmågor eller funktioner inom organisationen.
HEMLIG/SECRET Förkortning: H/S	1. Hemliga uppgifter vars röjande kan medföra betydande men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har försetts med beteckningen SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.	Konsekvenserna är allvarliga, av stor omfattning eller av väsentlig art och innebär ett direkt hot, om än mot avgränsade förmågor eller funktioner inom organisationen.

Informationssäkerhetsklass	Betydelse	Konsekvensbeskrivning
HEMLIG/CONFIDENTIAL Förkortning: H/C	1. Hemliga uppgifter vars röjande kan medföra ett inte obetydligt men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har försetts med beteckningen CONFIDENTIAL eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.	Förväntade konsekvenser är inte obetydliga och äventyrar, vållar skada, hindrar, underlättar, innebär större avbrott samt medför påtagliga negativa effekter om än i begränsad omfattning.
HEMLIG/RESTRICTED Förkortning: H/R	1. Hemliga uppgifter vars röjande kan medföra endast ringa men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har försetts med beteckningen RESTRICTED eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.	Förväntade konsekvenser är ringa och begränsas till att påverka, försvåra, hindra, undergräva, misskreditera eller störa verksamheten i mindre omfattning.

Informationssäkerhetsklass är en beteckning som anger hur uppgifter ska *hanteras* för att ett tillräckligt säkerhetsskydd ska erhållas.

Hemliga uppgifter ska placeras i informationssäkerhetsklass på grund av att uppgifterna omfattas av sekretess enligt OSL och rör rikets säkerhet. Hemliga uppgifter ska enligt säkerhetsskyddslagen ges ett säkerhetsskydd.

Placering av en uppgift eller en handling i informationssäkerhetsklass ska göras utifrån uppgiftens eller handlingens bedömda betydelse för Sveriges samlade försvarsåtgärder, alltså betydelsen för totalförsvaret i dess helhet.[84] Med hänsyn till det militära försvarets betydelse är det lämpligt att bedömningen görs med utgångspunkt i Försvarsmaktens samlade försvarsåtgärder.

84 Följer av de beskrivna betydelserna under punkterna 1 i 1 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd.

För att stärka skyddet för *utrikesklassificerade uppgifter* har Försvarsmakten beslutat Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar. I enlighet med dessa föreskrifter ska en utrikesklassificerad uppgift eller handling, så långt som möjligt, ha ett skydd som motsvarar vad som gäller för en hemlig uppgift och handling enligt:

- Försvarsmaktens föreskrifter om säkerhetsskydd,[85]
- Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel[85] samt
- Försvarsmaktens interna bestämmelser om IT-säkerhet.[86]

Utrikesklassificerade uppgifter och handlingar ska därför placeras i informationssäkerhetsklass.

Uppgifter som omfattas av sekretess men som inte är hemliga eller utrikesklassificerade, benämns *sekretessklassificerade uppgifter*. Uppgifter i denna sekretesskategori ska inte placeras i informationssäkerhetsklass, eftersom uppgifterna varken är hemliga eller utrikesklassificerade.

I H Säk Sekrbed A finns ytterligare beskrivning av informationssäkerhetsklasserna och tillvägagångssättet för hur hemliga och utrikesklassificerade uppgifter ska placeras i informationssäkerhetsklass.

6.5 Stöd för informationsklassificering

H Säk Sekrbed A beskriver informationsklassificering i Försvarsmakten. I handboken beskrivs offentlighet och sekretess i det allmännas verksamhet, fem sekretessbestämmelser som förekommer i Försvarsmaktens verksamhet, tillvägagångssättet för hur vissa uppgifter ska placeras i informationssäkerhetsklass samt rutinerna vid ärenden som rör begäran om att få ta del av en allmän handling i Försvarsmakten och utlämnande av dessa.

Del B av handboken består av skrivelser med detaljerade beskrivningar av informationsklassificeringen av uppgifter inom olika verksamhetsområden i Försvarsmakten.

85 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

86 1 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

6.6 Riktlinjer för informationsklassificering

Den som skapar information genom att upprätta en handling eller på annat sätt sammanställer uppgifter ansvarar även för informationsklassificeringen av uppgifterna.[87] Detta ansvar hindrar inte att t.ex. central verksamhetsutövare eller chef för organisationsenhet beslutar om riktlinjer för informationsklassificering som ett stöd för personalens bedömning av uppgifterna. Sådana riktlinjer kan vara ett resultat av den säkerhetsanalys som varje organisationsenhet ska genomföra för att identifiera vilka uppgifter som ska hållas hemliga med hänsyn till rikets säkerhet.[88] Sådana riktlinjer kan vara mer detaljerade än H SÄK Sekrbed B eller omfatta ett snävare område än vad H SÄK Sekrbed B gör, t.ex. uppgifter som rör viss materiel, en viss organisation eller ett specifikt internationellt samarbete.

Om riktlinjer för informationsklassificering beslutas, t.ex. av en sakområdesansvarig eller chef för organisationsenhet, bör säkerhetskontoret vid MUST orienteras om riktlinjerna så att den militära säkerhetstjänsten kan tillvarata verksamhetens säkerhetsintressen, t.ex. som underlag för H SÄK Sekrbed B.

6.7 Mission Secret i internationell verksamhet

Begreppet Mission Secret avser information som är kopplad till en specifik internationell insats och som kan förekomma i samtliga motsvarigheter till de svenska informationssäkerhetsklasserna (och inte enbart i nivån SECRET). Det som styr omfattningen av skyddsåtgärder för information avgörs uteslutande av uppgifternas informationsklassificering. För uppgifter som kräver skyddsåtgärder vilka motsvaras av det svenska kravet på säkerhetsskydd, framgår sådana krav genom uppgifternas placering i motsvarigheten till våra informationssäkerhetsklasser (som t.ex. NATO SECRET, NATO/ISAF CONFIDENTIAL, RESTREINT UE osv.).

I diskussioner framförs det ibland att man inom olika internationella organisationer (framförallt Nato) har ett begrepp, Mission Secret, som antyder att det på grund av sekretessens geografiska eller tidsmässiga begränsning inte behövs lika omfattande skyddsåtgärder för informationen. Detta synssätt är emellertid felaktigt.

Den enda självständiga betydelse som begreppet har är kopplat till delgivning av informationen. Information som är Mission Secret får, under vissa förutsättningar, delges efter beslut av den internationella insatsens befälhavare (Force Commander) istället för den normala och mer formella beslutsgången för delgivning av information inom Nato-systemet [referens 41].

87 Avsnitt 1.3 i H Säk Sekrbed A.

88 1 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

7 Behörighet

Med *behörighet att ta del av en uppgift* avses rättigheten att få ta del av uppgiften först efter att vissa villkor har uppfyllts. Villkoren kan vara olika för olika typer av uppgifter.

7.1 Behörighet att ta del av hemliga uppgifter

> ***Om inte något annat följer av bestämmelser i lag, är endast den behörig att ta del av hemliga uppgifter som:***
>
> ***1. bedöms pålitlig från säkerhetssynpunkt,***
>
> ***2. har tillräckliga kunskaper om säkerhetsskydd, och***
>
> ***3. behöver uppgifterna för sitt arbete i den verksamhet där de hemliga uppgifterna förekommer.***
>
> 7 § säkerhetsskyddsförordningen

Föreskriften gäller endast för hemliga uppgifter. Undantag från denna huvudregels tre villkor är om det av en bestämmelse i lag följer annat. Ett exempel på ett sådant undantag är om det av en bestämmelse i lag framgår att det finns en uppgifts- eller informationsskyldighet mellan myndigheter, t.ex. vid tillsyn eller brottsutredning. I sådana fall är personer som ska ta del av de hemliga uppgifterna behöriga att ta del av dem utan att villkoren om lämplighet ur säkerhetssynpunkt, tillräckliga kunskaper om säkerhetsskydd eller att personen ska behöva uppgifterna i den verksamhet där uppgifterna förekommer är uppfyllda. Märk väl att uppgifterna fortfarande är hemliga.

Hemliga uppgifter ska i den utsträckning det är möjligt förbehållas personer som har ett tjänstemässigt behov av att känna till dem och som har bedömts som lämpliga och pålitliga.[89] En överdriven tillämpning av villkoren för behörighet kan dock leda till att uppgifter inte kommer de personer till del som behöver dem för sitt arbete och medföra negativa konsekvenser för verksamheten.

Skyddsåtgärder för att säkerställa att behörighetskravet uppfylls behöver finnas för alla former av hemliga uppgifter och vara likvärdigt genomförd. En person som p.g.a. att behörighetskravet inte är uppfyllt inte kan ta del av en viss pappershandling ska heller inte kunna ta del av motsvarande elektroniska handling i ett IT-system (se även avsnitt 13.3).

Vad som i Försvarsmakten avses med *tillräckliga kunskaper om säkerhetsskydd* framgår i Instruktion avseende kunskapskrav säkerhetstjänst [referens 42].

89 Sidan 75, Säkerhetsskydd prop. 1995/96:129.

7.2 Behörighet att ta del av utrikesklassificerade uppgifter

Endast den är behörig att ta del av utrikesklassificerade uppgifter som

1. bedöms pålitlig från säkerhetssynpunkt,

2. har tillräckliga kunskaper om hur uppgifterna ska skyddas, och

3. behöver uppgifterna för sitt arbete i den verksamhet där uppgifterna förekommer.

2 kap. 4 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Kravet på behörighet för att ta del av utrikesklassificerade uppgifter är i Försvarsmakten detsamma som för hemliga uppgifter. En skillnad är dock att utrikesklassificerade uppgifter främst förekommer i internationella samarbeten och att uppgifterna normalt delges mellan de stater som ingår i samarbetet.

Föreskriften gäller endast inom Försvarsmakten och gäller inte för personal från andra myndigheter som deltar i samarbeten med Försvarsmakten.[90]

Om det finns en uppgifts- eller informationsskyldighet mellan myndigheter går den före föreskriften.

7.3 Behörighet att ta del av H/TS

Hemliga och utrikesklassificerade uppgifter som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET är de mest skyddsvärda uppgifterna. Sådana uppgifter ska därför ges ett mer omfattande skydd än andra uppgifter. En del av säkerhetsskyddet är att begränsa vilka personer som kan ta del av uppgifterna. Endast personer som kan antas behöva sådana uppgifter får beslutas vara behöriga att ta del av dessa.[91] Om sådana uppgifter inte förekommer i den verksamhet som en person deltar i, ska personen inte beslutas vara behöriga att ta del av sådana uppgifter.

Ett beslut om vilka personer som är behöriga att få ta del av uppgifter som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET måste följas i hanteringen av pappershandlingar och lagringsmedier samt i IT-system. I fråga om pappershandlingar och lagringsmedier används normalt en behörighetsförteckning vid en expedi-

90 1 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

91 2 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd.

tion (se avsnitt 7.5). IT-system som är avsedda för behandling av uppgifter som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET behöver ha en teknisk funktion som motsvarar expeditionspersonalens behörighetsförteckning. Säkerhetsfunktionen för behörighetskontroll behöver därför ha sådana egenskaper att tilldelning av en persons läsbehörighet till en uppgift som är placerad i informationssäkerhetsklass HEMLIG/TOP SECRET inte är möjlig om personen inte är beslutad vara behörig att ta del av sådana uppgifter.

7.4 Behörighet att ta del av sekretessklassificerade uppgifter

Vem i Försvarsmakten som är behörig att ta befattning med sekretessklassificerade uppgifter ska, ur säkerhetssynpunkt, inte beslutas. Det är de arbetsuppgifter som den enskilde har inom ramen för sitt ordinarie arbete som styr om han eller hon får ta del av en sekretessklassificerad uppgift.

7.5 Beslut om behörighet - behörighetsförteckning

> *Varje myndighet skall besluta vem som är behörig att ta befattning med hemliga handlingar som är placerade i någon av informationssäkerhetsklasserna HEMLIG/CONFIDENTIAL, HEMLIG/SECRET respektive HEMLIG/TOP SECRET eller som på annat sätt får ta del av en hemlig uppgift. Ett sådant beslut skall dokumenteras.*
>
> 2 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd

Myndigheter och organisationsenheter i Försvarsmakten ska fatta beslut enligt föreskriften.[92] För Försvarsmakten ska beslutet även omfatta utrikesklassificerade handlingar och uppgifter.[93] För krigsförband ska den organisationsenhet där förbandet ingår fatta beslutet.[94]

För att en person ska beslutas vara behörig att ta del av hemliga uppgifter krävs att villkoren i 7 § säkerhetsskyddsförordningen är uppfyllda i fråga om att en person har bedömts *lämplig ur säkerhetssynpunkt* och har *tillräckliga kunskaper om säkerhetsskydd* och *behöver uppgifterna* i den verksamhet där uppgifterna förekommer. Motsvarande gäller i Försvarsmakten för utrikesklassificerade uppgifter (avsnitt 7.2). Vad som i

92 1 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
93 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.
94 Bilaga 2 till Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).

Försvarsmakten avses med *tillräckliga kunskaper om säkerhetsskydd* framgår i Instruktion avseende kunskapskrav säkerhetstjänst [referens 42].

Detta innebär t.ex. att en person som inte har tillräckliga kunskaper om hur de hemliga uppgifterna ska skyddas inte får beslutas vara behörig att ta befattning med hemliga handlingar. Beslut om behörighet behöver alltså fattas *efter* att säkerhetsprövning och utbildning i säkerhetsskydd har genomförts. Att låta en person ta del av hemliga uppgifter under en provanställning bör ske restriktivt. I de fall personen sedan tidigare är känd (t.ex. om personen har arbetat med motsvarande arbetsuppgifter vid en annan myndighet) och har tillräckliga kunskaper om säkerhetsskydd behöver en sådan restriktivitet inte tillämpas.

Ett dokumenterat beslut om behörighet kan bestå av en förteckning över de personer som är behöriga att ta del av hemliga uppgifter. Vem som beslutar om behörighet bör i Försvarsmakten framgå av arbetsordning eller motsvarande. Rätten att fatta sådana beslut får delegeras inom en organisationsenhet. En sådan behörighetsförteckning förvaras lämpligast vid en expedition, så att personalen där kan kontrollera behörighet mot förteckningen. Även den person som normalt lottar inkommande ärenden, t.ex. stabschefen, bör ha en kopia av behörighetsförteckningen.

Om en person som ska hämta en hemlig handling inte finns förtecknad på en aktuell behörighetsförteckning ska personen inte få handlingen, även om handlingen är lottad på personen eller om personen är angiven i handlingens sändlista. Motsvarande gäller även för ett lagringsmedium som innehåller eller är avsett att innehålla hemliga uppgifter.[95]

Det är särskilt viktigt från säkerhetssynpunkt att en behörighetsförteckning hålls aktuell. Således bör den fortlöpande uppdateras, t.ex. då anställningar påbörjas och avslutas. En lämplig ordning är att en gång per år besluta om en ny behörighetsförteckning. Behörighetsförteckningarna är allmänna handlingar och av betydelse för eventuella utredningar varför de ska arkiveras. En behörighetsförteckning ska inte gallras eftersom Riksarkivet inte har meddelat någon föreskrift om gallring för behörighetsförteckningar.

En behörighetsförteckning bör innehålla identifieringsuppgifter som består av namn och personnummer (födelsedatum är inte tillräckligt) samt uppgift om vilken högsta informationssäkerhetsklass som personen får ta del av. Om det behövs kan förteckningen även innehålla uppgift om vilka personer som får kvittera ut en hemlig handling, signaturer, handläggarkoder eller motsvarande.

95 7 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Särskild vikt bör läggas vid beslut om behörighet som avser en handling eller ett lagringsmedium som är placerad i informationssäkerhetsklass HEMLIG/TOP SECRET (avsnitt 7.3).

Något beslut behöver inte fattas för vem som är behörig att ta befattning med hemliga handlingar som är placerade i informationssäkerhetsklass HEMLIG/RESTRICTED. Med hänsyn till att en sådan handling alltjämt innehåller hemliga uppgifter får myndigheten endast, enligt 7 § säkerhetsskyddsförordningen, delge uppgifterna till den som är behörig att ta del av dem för sitt arbete i den verksamhet som uppgifterna förekommer. Något beslut behöver heller inte fattas om en person på något annat sätt (t.ex. muntligen) tar del av hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/RESTRICTED.

I Försvarsmakten behövs inget beslut om behörighet för att ta del av en sekretessklassificerad uppgift (avsnitt 7.4). En behörighetsförteckning ska därför inte upprättas för behörighet att ta del av sådana uppgifter.

7.5.1 Sekretess för uppgifter i en behörighetsförteckning

En underrättelseaktörs målsökning av personal underlättas om aktören har tillgång till en behörighetsförteckning som visar vilka personer som är behöriga att ta del av hemliga uppgifter. Då behörigheten att ta del av hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET normalt är begränsad inom en myndighet (avsnitt 7.3) bör sådana förteckningar omfattas av sekretess enligt 15 kap. 2 § OSL. Menet vid ett röjande av en förteckning är dock ringa då det endast underlättar en närmare målsökning varför förteckningarna bör placeras i informationssäkerhetsklass HEMLIG/RESTRICTED. Andra behörighetsförteckningar för hemliga och utrikesklassificerade uppgifter bör omfattas av sekretess enligt 18 kap. 8 § fjärde punkten OSL. I Försvarsmakten informationsklassificeras de som sekretessklassificerade handlingar.

7.6 Sekretess inom och mellan myndigheter

Huvudregeln är att sekretess enligt OSL även gäller mellan svenska myndigheter.[96] Dessutom gäller sekretess mellan olika verksamhetsgrenar inom en myndighet om de är självständiga i förhållande till varandra.[97] I OSL finns flera bestämmelser som anger när sekretess *inte* är ett hinder för att sekretessbelagda uppgifter ska kunna lämnas till en annan myndighet. T.ex. om uppgiftsskyldighet följer av lag eller förordning,[98] om lämnande av en sekretessbelagd uppgift är nödvändigt för att den utlämnande

96 8 kap. 1 § OSL.
97 8 kap. 2 § OSL.
98 10 kap. 28 § första stycket OSL.

myndigheten ska kunna fullgöra sin verksamhet,[99] eller om en sekretessbelagd uppgift behövs för tillsyn över den myndighet där uppgiften förekommer.[100] Sekretessen hindrar inte heller att en sekretessbelagd uppgift lämnas till riksdagen eller regeringen.[101] Den s.k. generalklausulen i OSL ger en myndighet möjlighet att i vissa fall lämna en sekretessbelagd uppgift till en annan myndighet, eller annan verksamhetsgren inom samma myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.[102]

I de fall sekretess enligt OSL *hindrar* att en uppgift ska delges en person vid en annan myndighet eller inom en myndighet kan den personen inte vara behörig att ta del av uppgiften. Föreskrifterna i OSL har t.ex. företräde framför 7 § säkerhetsskyddsförordningen om behörighet att ta del av hemliga uppgifter.

7.7 Behörighet för personal vid utländsk myndighet

En uppgift för vilken sekretess gäller enligt denna lag får inte röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte

1. utlämnande sker i enlighet med särskild föreskrift i lag eller förordning, eller

2. uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

8 kap. 3 § OSL

Sekretessen enligt OSL gäller även gentemot utländska myndigheter och mellanfolkliga organisationer. I internationell verksamhet kan det finnas ett behov av att delge en uppgift som omfattas av sekretess enligt OSL till personal från en utländsk myndighet eller mellanfolklig organisation. Sådan delgivning är endast tillåten om villkoren i föreskriften är uppfyllda.

Observera att det av andra punkten framgår att delgivningen ska vara förenlig med svenska intressen, t.ex. Sveriges intresse av internationellt samarbete med den utländska myndigheten eller mellanfolkliga organisationen. Myndighetens prövning ska ske

99 10 kap. 2 § OSL.
100 10 kap. 17 § OSL.
101 10 kap. 15 § OSL.
102 10 kap. 27 § OSL.

av myndighetens chef eller den person han eller hon har delegerat beslutsrätten till, t.ex. genom arbetsordning.

Förutom denna generella reglering finns särskilda villkor för delgivning av en uppgift som omfattas av sekretess enligt 15 kap. 2 § OSL. En sådan uppgift får av Försvarsmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut lämnas till en utländsk myndighet som deltar i ett samarbete inom Försvarsdepartementets område *endast* om samtliga följande fyra villkor är uppfyllda.

1. Samarbetet ska ingå i överenskommelse med den andra staten eller mellanfolkliga organisationen som har ingåtts av regeringen eller en förvaltningsmyndighet efter uppdrag från regeringen.
2. Det är enligt den utlämnande myndighetens prövning nödvändigt för att genomföra samarbetet.
3. Uppgiften är inte av synnerlig betydelse för rikets säkerhet (kvalificerat hemlig).
4. Uppgiften kan inte ge underlag för utveckling av motmedel mot Sveriges försvarssystem.[103]

Om samtliga villkor är uppfyllda behöver inte regeringen tillfrågas före ett lämnande av en uppgift. Om det i Försvarsmakten finns ett behov av delgivning av sekretessbelagda uppgifter som inte är möjlig med hänsyn till villkoren ovan bör juridiska staben i Högkvarteret kontaktas.

Personal vid en utländsk myndighet eller mellanfolklig organisation som ska ges tillgång till informationstillgångar får endast beslutas vara behörighet att ta del av sekretessbelagda uppgifter om villkoren ovan är uppfyllda. Administrativa rutiner för hantering av pappershandlingar och lagringsmedier (t.ex. lottning av ärenden och åtkomst till förvaringsutrymmen) måste därför utformas så att den utländska personalen endast kan komma åt de uppgifter som de har beslutats vara behöriga till.

I de fall den utländska personalen ska vara användare av ett IT-system som en svensk myndighet tillhandahållit måste säkerhetsfunktionen för behörighetskontroll användas så att den utländska personalen endast kan komma åt de uppgifter som de har beslutats vara behöriga till. IT-system ger potentiellt tillgång till en stor mängd uppgifter varför frågan om styrning av behörigheter är av stor vikt. Se även avsnitt 15.1.3 om utländsk personals användning av Försvarsmaktens IT-system.

Att personal från en utländsk myndighet har beslutats vara behöriga att ta del av en sekretessbelagd uppgift innebär inte att personal från en tredje stat är behörig att ta del

103 1 § förordningen om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet.

av uppgiften, det kan t.o.m. vara icke önskvärt beroende på det intresse som sekretessen ska skydda.

De begränsningar som finns för delgivning av uppgifter som omfattas av sekretess enligt 15 kap. 2 § OSL finns inte för *utrikesklassificerade* uppgifter. Det är t.ex. möjligt att delge en utrikesklassificerad uppgift som är placerad i informationssäkerhetsklass HEMLIG/TOP SECRET om villkoren i 8 kap. 3 § OSL är uppfyllda.

Om en *hemlig* uppgift inte får lämnas till en annan stat eller mellanfolklig organisation kan inte heller uppgiften skyddas med tekniska skyddsåtgärder som den andra staten eller mellanfolkliga organisationen har kontroll över. En sådan uppgift kan t.ex. inte förvaras i ett förvaringsutrymme som tillhandahållits av den andra staten eller mellanfolkliga organisationen. För att en sådan uppgift ska få behandlas i ett IT-system som tillhandahålls av den andra staten eller mellanfolkliga organisationen ska IT-systemet först ackrediteras av den svenska myndighet som lämnar uppgiften. Det kan dock vara svårt att säkerställa att den hemliga uppgiften inte obehörigen röjs, ändras eller förstörs i ett sådant IT-system. På motsvarande sätt kan det finnas stora svårigheter att visa att en sådan hemlig uppgift som ska krypteras med krypto som tillhandahållits av den andra staten eller mellanfolkliga organisationen ges ett tillräckligt skydd av kryptot.

7.8 Begränsning i att delge eller använda en handling

Har en utländsk myndighet eller mellanfolklig organisation försett en hemlig handling med en anteckning som innebär begränsningar i att delge eller använda handlingen ska anteckningen följas om hinder inte möter enligt svensk rätt.

9 kap. 5 a § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

I bilaterala säkerhetsskyddsavtal förekommer det ofta ett åtagande att en part som delger information till en annan part kan specificera för vilket ändamål som informationen ska användas. En sådan specificering, som kan ske genom anteckning på en handling eller i någon form av styrande dokument, ska naturligtvis följas i den mån det inte strider mot svensk rätt att följa specificeringen. Detta innebär att om informationen är delgiven unikt för ett visst materielsamarbete får informationen inte användas i något annat sammanhang. Naturligtvis bestämmer myndigheten (utifrån behörighetsrekvisiten) vilka vid myndigheten som ska delges informationen och bestämmelsen i sig avser inte att begränsa detta på något sätt.

En anteckning som innebär *begränsningar i att delge eller använda handlingar* benämns i internationella sammanhang normalt *caveat*. Benämningen kan även användas i andra områden än informationssäkerhet och har då andra betydelser. Exempel på caveat är:

Mellanfolklig organisation	Caveat
EU	RELEASABLE TO NBG PARTICIPANTS
EU	RELEASABLE TO NATO
EU	RELEASABLE TO NORWAY
NATO	RELEASABLE TO NATO MEMBER AND SWEDEN AND IRELAND ONLY
NATO	RELEASABLE TO THE EU

Om en allmän handling som är försedd med en sådan angiven begränsning begärs ut måste naturligtvis sekretessen vägas mot offentlighetsintressena. Om en sådan handling inte innehåller någon uppgift som omfattas av sekretess enligt OSL inträffar ett fall där den angivna begränsningen får vika för svensk rätt. Detta kan naturligtvis få betydelse för Sveriges relationer med det upprättande landet, varför sekretessprövningen måste vara mycket noggrann i detta fall. Anteckningen om caveat innebär ofta att handlingen ska sekretessbeläggas enligt 15 kap. 1 § OSL, den s.k. utrikessekretessen, men anteckningen om caveat på handlingen innebär inte i sig att sekretess föreligger.

Något generellt regelverk för att förse svenska handlingar med caveat saknas. Om en svensk handling som har överlämnas till en annan stat saknar märkning om caveat gäller ändå grundprincipen att mottagarlandet inte utan uttryckligt godkännande får delge hemliga och utrikesklassificerade uppgifter till tredje part. Detta följer av de internationella säkerhetsskyddsöverenskommelserna som Sverige har ingått.

Föreskrifter om märkning med caveat som gäller för handlingar som ska lämnas till en annan stat eller mellanfolklig organisation saknas i Försvarsmakten. I internationella samarbeten får stöd för märkning med caveat sökas i de regelverk som styr respektive samarbete.

7.9 Intyg om säkerhetsklarering

Innan en företrädare för en utländsk myndighet eller en mellanfolklig organisation tar del av hemliga uppgifter ska chefen för den organisationsenhet som tillhandahåller uppgifterna, eller den han eller hon bestämmer se till att företrädaren uppvisar ett intyg om säkerhetsklarering, som är utfärdat av behörig myndighet eller mellanfolklig organisation, och som innebär att företrädaren får ta del av uppgifterna.

Vad som anges i första stycket behöver inte iakttas om det är uppenbart obehövligt.

2 kap. 2 a § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

I bilaterala säkerhetsskyddsavtal finns det vanligen bestämmelser om behörighet till information och hur en sådan behörighet ska styrkas. Behörighetsprincipen är densamma i många länder, men det som skiljer sig från svenska förhållanden är att andra länder normalt utfärdar ett intyg som styrker en persons behörighet att ta del av hemliga uppgifter (eller motsvarande typ av information i de andra länderna). I Sverige har vi anpassat oss till denna modell när det behövs och vi har även åtagit oss i dessa avtal att följa rutinerna kring uppvisande av intyg om säkerhetsklarering (på engelska *Certificate of Personnel Security Clearance*, PSCC eller vanligare bara PSC).

Intyget kan antingen uppvisas personligen eller skickas av den organisation som personen företräder eller av en nationell säkerhetsmyndighet. Det förekommer också att denna behörighet intygas som en del i en besöksanmälan. Således behöver inte intyget följa en särskild mall, även om sådana kan underlätta intygandet. Alla dessa sätt är möjliga, men det är chefen för den organisationsenhet där de hemliga uppgifterna ska delges som ansvarar för att personen i fråga verkligen har ett intyg i någon form. Vid osäkerhet kring utformningen av ett sådant intyg eller avseende utfärdaren bör samverkan ske med säkerhetskontoret vid MUST. I vissa särskilda samarbeten förekommer det att ett utbyte av hemliga uppgifter föregås av noggranna förberedelser samt att namn på behöriga personer skickas i förväg via särskilt överenskomna kanaler. I sådana särskilda fall där det är uppenbart att en person som representerar en utländsk myndighet har behörighet till hemliga uppgifter i en viss informationssäkerhetsklass kan detta underlåtas under förutsättning att det också är accepterat, och tillämpas ömsesidigt, av den utländska myndigheten.

Ett intyg om säkerhetsklarering innebär inte att den utländska företrädaren med automatik ska få ta del av uppgifter som omfattas av sekretess enligt OSL (avsnitt 7.7). Vid osäkerhet om en utländsk företrädare får ta del av uppgifter som omfattas av sekretess enligt OSL bör samverkan ske med juridiska staben i Högkvarteret eller med MUST.

7.10 Principer för behörighetstilldelning

Två grundläggande principer finns för behörighetstilldelning. Den första kan kallas *sluten behörighetstilldelning* där en persons behörighet att ta del av en specifik sekretessbelagd uppgift, eller handling där sådan uppgift ingår i, beslutas i varje enskilt fall. För en pappershandling kan ett sådant beslut t.ex. ske i form av lottning, där mottagaren av handlingen bestäms av den som lottar handlingen. I fråga om muntlig delgivning av sekretessbelagda uppgifter bestäms behörigheten till uppgifterna av vilka personer som deltar och som, ofta underförstått, i förväg ha bedömts ha ett behov av uppgifterna. I IT-system kan sluten behörighetstilldelning t.ex. ske genom att sända e-post med en sekretessbelagd uppgift eller genom att ändra IT-systemets inställningar för behörighetskontroll så att ytterligare en person kan ta del av en sekretessbelagd uppgift.

Den andra principen kan kallas *öppen behörighetstilldelning* där en eller flera personer ges möjlighet att ta del av sekretessbelagda uppgifter utan att det finns ett omedelbart behov av uppgifterna. För att en öppen behörighetstilldelning ska kunna komma i fråga måste det förutsättas att personerna kommer ha ett behov av uppgifterna, t.ex. vid en uppkommen händelse. Personerna kan genom egna åtgärder själv söka och ta del av de sekretessbelagda uppgifterna, t.ex. i ett IT-system eller ett förvaringsutrymme för handlingar.

Öppen behörighetstilldelning kan vara lämplig för sekretessbelagda uppgifter som ingår i en avgränsad samling uppgifter och kan endast komma i fråga för personer som ingår i den verksamhet där uppgifterna förekommer. Exempel på användning av öppen behörighetstilldelning kan vara när en analytiker behöver ha tillgång till ett stort antal rapporter för att självständigt värdera information, dra slutsatser och formulera hypoteser. Ett andra exempel kan vara personal som tjänstgör i en ledningscentral och där behöver tillgång till uppgifter med hänsyn till uppkomna händelser. Ett tredje exempel är inom sjuk- och hälsovården där flera personer i verksamheten behöver ha en möjlig åtkomst till patientjournaler. Där denna typ av behörighetstilldelning används förekommer det ofta en aktiv uppföljning på hur användarna sköter det förtroende de har tilldelats. Uppföljningen kan bestå i en aktiv övervakning som söker tecken på att en användare gör sökningar vilka han eller hon inte behöver göra i sin tjänst.

För merparten av Försvarsmaktens informationstillgångar som består av hemliga och utrikesklassificerade uppgifter är sluten behörighetstilldelning den lämpligaste principen för behörighetstilldelning. Det kan dock finnas verksamheter och informationstillgångar där den slutna behörighetstilldelningen skulle medföra stora begränsningar och effektivitetsförluster. I sådana verksamheter och för sådana informationstillgångar kan en öppen behörighetstilldelning vara aktuell.

I en bedömning av lämpligheten av en öppen behörighetstilldelning får de positiva effekterna för verksamheten vägas mot behovet av en öppen behörighetstilldelning, de eventuella skador som ett röjande kan ge och antalet personer som avses vara behöriga. Det kan t.ex. vara olämpligt att för hundratals personer tillämpa en öppen behörighetstilldelning på uppgifter som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET.

En person kan ha tillgång till flera informationstillgångar där de två principerna kan tillämpas olika. Att en person genom en öppen behörighetstilldelning har tillgång till en informationstillgång innebär inte att en öppen behörighetstilldelning ska tilllämpas på alla andra informationstillgångar som personen behöver ha tillgång till.

Behov av och bedömning av lämplighet av en öppen behörighetstilldelning i IT-system dokumenteras i IT-systemets säkerhetsmålsättning (avsnitt 14.1).

Då en öppen behörighetstilldelning innebär en större risk för informationsförluster behöver risken kompenseras med en mer frekvent och noggrannare uppföljning av vilka uppgifter som personerna tar del av. En sådan uppföljning kan för IT-system bl.a. utformas så att en persons närmaste chef regelbundet får automatiskt genererade rapporter om vilka sökningar som personen har genomfört och handlingar som personen har tagit del av.

Gemensam användning av hemliga handlingar (avsnitt 9.15.1) är ett exempel på användning av principen *öppen behörighetstilldelning*.

7.11 Nödöppning

Vid en nödsituation kan en person ha ett behov av tillgång till informationstillgångar som personen normalt inte har åtkomst till. I sådana fall där det inte är möjligt att genom ordinarie rutiner ge personen åtkomst till informationstillgången används *nödöppning*. Nödöppning kan t.ex. ske genom öppning av förvaringsutrymme med hjälp av reservkod. I IT-system kan det vara tekniska funktioner som när de används ger personen rättighet att läsa, ändra, påverka uppgifter eller använda funktioner i IT-systemet. Nödöppning bör vara beslutad av en chef, ske i närvaro av en person som bevittnar händelsen och dokumenteras i en logg som bevaras. En verksamhets behov av nödöppning i IT-system måste framgå i säkerhetsmålsättningen för IT-systemet (avsnitt 14.1).

Nödsituation avser inte endast situationer där en fara hotar liv, hälsa, egendom eller något annat viktigt av rättsordningen skyddat intresse.[104] Det kan även vara fråga om att en anställds frånvaro (t.ex. sjukdom eller längre tids ledighet) hindrar verksamhet.

104 24 kap. 4 § brottsbalken.

Om nödöppning är lämpligt ur säkerhetssynpunkt får bedömas inom ramen för auktorisation, ackreditering och kontroll.

I Försvarsmakten finns föreskrifter om när kod eller en reservnyckel till ett förvaringsutrymme som används för förvaring av hemliga handlingar får användas av någon annan än den som har ansvar för förvaringsutrymmet.[105]

7.12 Behörighetssystem

I vissa säkerhetskänsliga verksamheter kan det finnas ett behov av att ytterligare styra vem som är behörig att ta del av uppgifterna som förekommer i verksamheten. En sådan styrning uppnås med formella behörighetssystem. Innan en person ska ta del av en uppgift som rör verksamheten ska personen beslutas vara behörig att få ta del av uppgifter i den verksamheten. Behörighetssystem är en skyddsåtgärd som inte går före föreskrifter i OSL om bl.a. sekretess inom och mellan myndigheter eller föreskriften om behörighet i 7 § säkerhetsskyddsförordningen.

Ett behörighetssystem medför ytterligare svårigheter att hantera de informationstillgångar som omfattas av ett sådant system varför det endast ska användas för hemliga uppgifter som har ett mycket starkt skyddsbehov.

Användningen av ett behörighetssystem kan innebära att andra rutiner, än de som används för beslut om vem som är behörig att ta del av andra hemliga uppgifter, ska användas. Hur ett behörighetssystem ska användas ska normalt framgå i en författning om säkerhetsskydd. Om behörighetssystemet ska användas vid flera myndigheter ska användningen styras i en författning som gäller för myndigheterna.

Att behörighetssystem finns kan väcka uppmärksamhet om förhållanden som med hänsyn till rikets säkerhet ska hållas hemliga och därför ska skyddas mot obehörig insyn. Även uppgiften om vem som är, eller har varit, behörig enligt ett behörighetssystem är en uppgift som vanligtvis omfattas av sekretess enligt 15 kap. 2 § OSL. Personer som är beslutade att vara behöriga enligt ett behörighetssystem ska inte tala om det utanför den verksamhet som behörighetssystemet gäller för. Även inom sådana verksamheter kan det finnas ytterligare begränsningar.

Säkerhetskontoret vid MUST hanterar ärenden som rör behörighetssystem.

105 3 kap. 10 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

7.13 Restriktiv behörighet

Restriktiv behörighet är en begränsning av möjligheten för behöriga personer att för en specifik uppgift eller handling ge ytterligare personer behörighet att ta del av uppgiften eller handlingen. Detta kan vara lämpligt i fråga om mycket känsliga uppgifter i IT-system där en berättigad skyddsåtgärd är att snävt begränsa vilka personer som kan ta del av uppgiften.

Något generellt regelverk för restriktiv behörighet saknas. En handling som innehåller anteckningen RESTRIKTIV BEHÖRIGHET eller liknande behöver därför inte följas. Skyddseffekten av skyddsåtgärden är således liten utanför en verksamhet eller IT-system där detta tillämpas.

7.14 Behörighet att ändra uppgifter

Styrning av behörighet behöver inte enbart avse möjligheten att ta del av sekretessbelagda uppgifter utan kan även avse möjligheten att ändra eller förstöra uppgifter. Skyddet mot att obehörigen ta del av sekretessbelagda uppgifter ger även indirekt ett skydd mot ändring av uppgifterna. Att en person är beslutad att vara behörig att ta del av en sekretessbelagd uppgift innebär dock inte att personen ska få ändra uppgiften.

Informationssäkerhet för hemliga uppgifter ska även förebygga en obehörig ändring eller förstöring av sådana uppgifter.[106] Behov av skydd mot obehörig ändring eller förstöring av uppgifter ska även analyseras för ett IT-system som inte är avsett för behandling av hemliga uppgifter.[107] Även uppgifter som inte omfattas av sekretess behöver normalt ges ett skydd mot obehörig ändring. Säkerhetsfunktionen behörighetskontroll i IT-system ska därför även användas för att ge de behandlade uppgifterna ett skydd mot obehörig ändring. På motsvarande sätt är säkerhetsfunktionen säkerhetsloggning även avsedd för registrering av händelsen att en uppgift har ändrats, om en sådan händelse är av betydelse för säkerheten i IT-systemet.[108] [109]

Behovet av styrning av behörighet för att ändra uppgifter måste uppmärksammas i en säkerhetsmålsättning för IT-systemet (avsnitt 14.1).

106 7 § 1 säkerhetsskyddslagen.
107 4 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
108 7 kap. 1 § 5 Försvarsmaktens föreskrifter om säkerhetsskydd.
109 1 kap. 6 § 8 Försvarsmaktens interna bestämmelser om IT-säkerhet.

8 Sekretessbevis

8.1 Hemliga uppgifter

Den som tillåts ta del av hemliga uppgifter skall upplysas om räckvidden och innebörden av sekretessen.

8 § säkerhetsskyddsförordningen

Med räckvidden för sekretessen avses t.ex. att sekretessen gäller inom myndigheten och mellan myndigheter samt att sekretessen gäller efter avslutad anställning eller motsvarande. Med innebörden av sekretessen avses de fall där en viss sekretessbestämmelse ska tillämpas för ett visst förhållande, t.ex. i vilka fall uppgifter i verksamheten är sekretessbelagda enligt 15 kap. 2 § OSL.

Chef för organisationsenhet, eller den han eller hon bestämmer, ska se till att den som får ta del av hemliga uppgifter har upplysts om räckvidden och innebörden av sekretessen och att ett bevis (sekretessbevis) upprättas om att så har skett.

2 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Sekretessbeviset tecknas först efter att upplysningen har ägt rum. Upplysningen bör genomföras av en person som har kunskap om sekretessbestämmelserna och som kan förklara deras innebörd. Det är således inte tillräckligt att få läsa sekretessbestämmelsernas innehåll utan att de förklaras.

Ett sekretessbevis är en bekräftelse på att personen har blivit informerad om vad som gäller om sekretess. Att en person undertecknar ett sekretessbevis binder inte personen ifråga om sekretess. En anställd är bunden av sekretessbestämmelserna i OSL oavsett om ett sekretessbevis har undertecknats. I en eventuell rättegång är ett sekretessbevis ett bevis på att den anställde har eller borde ha förstått att han eller hon bröt mot sin tystnadsplikt. Då någon bryter mot tystnadsplikten kan personen, enligt 20 kap. 3 § brottsbalken, dömas till böter eller fängelse i högst ett år för brott mot tystnadsplikt.

Bilaga 3 innehåller en förteckning med hänvisningar till blanketter, där bl.a. sekretessbevis är medtagen.

Sekretessbevis får endast upprättas för personer som är anställda vid myndigheten, har uppdrag vid myndigheten eller på grund av tjänsteplikt deltar i myndighetens verksamhet. Sekretessbevis får inte upprättas för en annan myndighets personal då skyddsåtgärden inte är reglerad i en myndighetsöverskridande författning. Det får förutsättas att personal från en annan myndighet har undertecknat ett sekretessbevis vid den myndighet där personalen är anställd. Det kan i samarbeten mellan myndigheter vara nödvändigt att *upplysa* den deltagande personalen om vilka uppgifter i samarbetet som bedöms omfattas av sekretess. En sådan upplysning kan genomföras utan att sekretessbevis upprättas.

Sekretessbevis ska bevaras, någon gallring av sekretessbevis är inte tillåten. Detta då tystnadsplikten inte är tidsbegränsad [referens 19].

8.2 Utrikesklassificerade uppgifter

Sekretessbevis ska på samma sätt som för hemliga uppgifter användas för utrikesklassificerade uppgifter.[110] Endast ett sekretessbevis ska användas, det finns ingen anledning att olika sekretessbevis ska användas för hemliga respektive utrikesklassificerade uppgifter.

8.3 Sekretessklassificerade uppgifter

> *Chef för organisationsenhet ska se till att den som tillåts ta del av sekretessklassificerade uppgifter ska upplysas om räckvidden och innebörden av sekretessen.*
>
> 3 kap. 3 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Den som får ta del av sekretessklassificerade uppgifter ska ha upplysts om innebörden och räckvidden av sekretessen.

Det finns inget krav på att sekretessbevis ska ha upprättats innan personal i Försvarsmakten får ta del av sekretessklassificerade uppgifter. Sekretessbevis ska därför inte upprättas för sådana uppgifter. En upplysning om räckvidden och innebörden av sekretessen kan vad gäller sekretessklassificerade uppgifter äga rum under utbildning av personal. Det är nödvändigt att en sådan utbildning anpassas för vilka typer av sekretessklassificerade uppgifter som personalen ska ta del av. Personal i FMLOG som

110 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

ska arbeta med transport eller förvaring av vapen, ammunition eller sprängämnen kan t.ex. utbildas i sekretess för säkerhets- eller bevakningsåtgärd enligt 18 kap. 8 § OSL.

8.4 Sekretessavtal i privat verksamhet

I privat näringsverksamhet är det inte ovanligt att personer som tillfälligt deltar i verksamheten eller som på annat sätt ska ges insyn i verksamheten får skriva under sekretessavtal (på engelska vanligen benämnt non-disclosure agreement). Ett sådant sekretessavtal är dock inte bindande för personal vid en myndighet som har att följa TF och OSL. Ett sådant sekretessavtal kan t.ex. inte ha företräde framför tjänstemäns meddelarfrihet. När det gäller uppgifter om den privata verksamheten som förekommer i en myndighet kan uppgifterna omfattas av sekretess enligt OSL. För övriga uppgifter som inte träffas av en sekretessbestämmelse i OSL gäller inte sekretess.

En anställd i Försvarsmakten bör inte skriva under ett sekretessavtal med hänvisning till att avtalet inte är giltigt för den anställde eller Försvarsmakten. Beroende på situationen kan det dock vara nödvändigt att skriva under för att inte försena den pågående verksamheten.

9 Hantering av handlingar

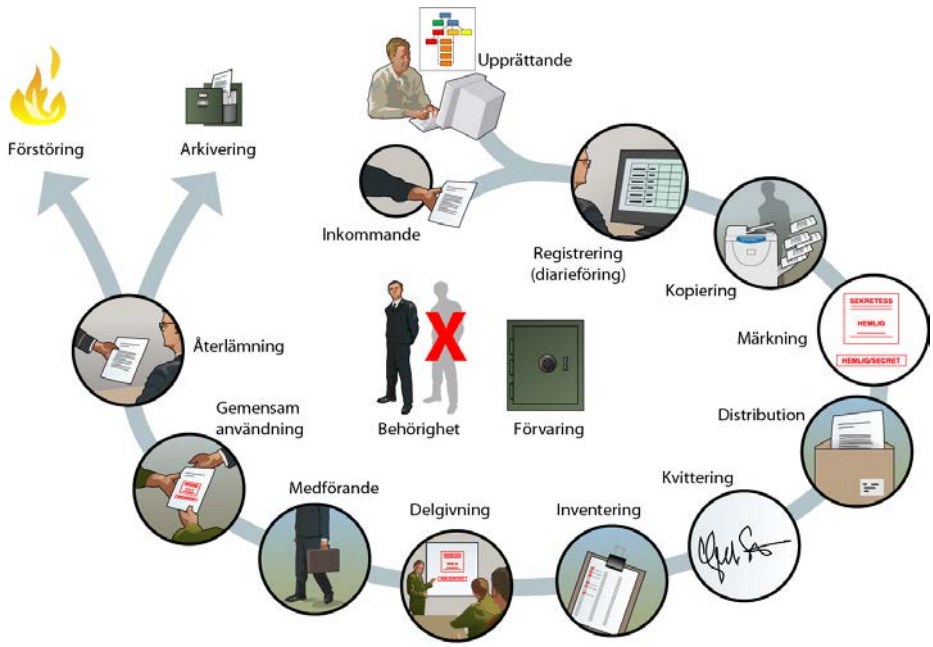


Bild 9:1 – En handlings livscykel och skyddsåtgärder under livscykeln.

Bild 9:1 visar en handlings livscykel och skyddsåtgärder i Försvarsmakten under livscykeln. Livscykelns delar och skyddsåtgärderna beskrivs nedan.

9.1 Inkommande handlingar

9.1.1 Sekretessmarkering av inkommande handlingar

En handling som inte är sekretessmarkerad ska sekretessmarkeras av Försvarsmakten om handlingen bedöms innehålla någon uppgift som omfattas av sekretess enligt OSL.[111] En förklaring till en sådan situation kan vara att det inte finns någon generell skyldighet för myndigheter att sekretessmarkera allmänna handlingar som innehåller någon uppgift som omfattas av sekretess enligt OSL, förutom i de fall uppgifterna rör rikets säkerhet.

En handling som skickas inom Försvarsmakten behöver endast sekretessmarkeras av den organisationsenhet där handlingen har upprättats. En organisationsenhet som tar

111 2 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd samt 2 kap. 3 § och 3 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

emot en sådan handling från en annan organisationsenhet behöver således inte sekretessmarkera handlingen då den redan är sekretessmarkerad av Försvarsmakten.

9.1.2 Handlingar från en annan myndighet

En handling som inkommer till Försvarsmakten får inte sekretessmarkeras (se om sekretessmarkering) utan att en sekretessbedömning har gjorts av uppgifterna i handlingen. En sådan sekretessbedömning får vara översiktlig och kan grundas på instruktioner från t.ex. stabschef eller de erfarenheter som finns vid expedition eller motsvarande. Sekretessmarkeringar beskrivs i avsnitt 9.5

En handling från en annan svensk myndighet som är sekretessmarkerad ska normalt sekretessmarkeras på nytt när handlingen kommer in till Försvarsmakten. Försvarsmakten är normalt inte skyldig att följa den avsändande myndighetens sekretessbedömning. I OSL finns föreskrifter om överföring av sekretess.

9.1.3 Handlingar som inkommer genom kryfax

Det bör poängteras att en handling inte får sekretessmarkeras utan att en sekretessbedömning är gjord av uppgifterna i handlingen, en sådan sekretessbedömning får vara översiktlig.

Handlingar som inkommer via kryfax sekretessmarkeras ofta utan att någon sekretessbedömning har gjorts. Således får inte enbart att en handling har överförts med kryfax utgöra grund för att sekretessmarkera handlingen. I de fall det råder oklarhet om en kryfaxhandling innehåller uppgifter som omfattas av sekretess enligt OSL eller inte bör avsändaren kontaktas. Naturligtvis får inte hemliga uppgifter överföras med ett sambandsmedel som inte är krypterat.

Kryfaxhandlingar från Utrikesdepartementet rör ofta Sveriges förbindelser med annan stat eller mellanfolklig organisation. Flertalet av dessa handlingar bedöms innehålla uppgifter som omfattas av sekretess enligt 15 kap. 1 § OSL. Sådana kryfaxhandlingar bör därför då de inkommer till Försvarsmakten sekretessmarkeras med hänvisning till 15 kap. 1 § OSL oavsett om de är sekretessmarkerade eller inte vid Utrikesdepartementet.

9.1.4 Handlingar från en annan stat eller mellanfolklig organisation

En inkommande handling från en annan stat eller en mellanfolklig organisation som är märkt med den statens eller organisationens motsvarighet till en informationssäkerhetsklass ska placeras i informationssäkerhetsklass om den staten eller den mellanfolkliga organisationen har märkt handlingen med en motsvarighet till informationssäkerhetsklass. En sådan handling innehåller normalt inte uppgifter som omfattas av

sekretess enligt 15 kap. 2 § OSL (s.k. försvarssekretess). Däremot omfattas uppgifterna i handlingarna sannolikt av sekretess enligt 15 kap. 1 § OSL (den s.k. utrikessekretessen). Då sådana handlingar sekretessmarkeras ska hänvisning således göras till 15 kap. 1 § OSL. En sådan handling är i Försvarsmakten *utrikesklassificerad*.

Förteckning över andra staters och mellanfolkliga organisationers motsvarighet till informationssäkerhetsklasser finns i bilaga 2 till H Säk Sekrbed A.

Det bör observeras att en handling som inkommer från en annan stat eller en mellanfolklig organisation naturligtvis kan innehålla uppgifter som omfattas av sekretess enligt OSL och röra rikets säkerhet. Det kan i samarbeten med andra stater och mellanfolkliga organisationer förekomma uppgifter som t.ex. omfattas av sekretess enligt 15 kap. 2 § OSL. I sällsynta fall kan även uppgifter som omfattas av sekretess enligt 15 kap. 1 § OSL röra rikets säkerhet. De är då hemliga uppgifter. Sådana handlingar är *hemliga* och ska placeras i informationssäkerhetsklass.

9.1.5 Handlingar från utlandet som är märkta UNCLASSIFIED

Handlingar från andra stater och mellanfolkliga organisationer kan vara försedda med beteckningar som anger att handlingen innehåller uppgifter som omfattas av sekretess enligt den andra statens eller mellanfolkliga organisationens regler men som inte ska ges ett särskilt skydd. Exempel på sådana beteckningar är NATO UNCLASSIFIED, LIMITE, som förekommer i EU, och Controlled Unclassified Information, som förekommer i USA.

En handling som inkommer till Försvarsmakten från en annan stat eller en mellanfolklig organisation och som är märkt UNCLASSIFIED eller motsvarande innehåller normalt inte uppgifter som omfattas av sekretess enligt 15 kap. 2 § OSL. Detta medför att handlingen inte ska placeras i en informationssäkerhetsklass och därmed inte ska ges ett säkerhetsskydd. Om det däremot kan antas att ett röjande av uppgifterna i handlingen stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar Sverige medför detta att handlingen bör sekretessmarkeras med en hänvisning till 15 kap. 1 § OSL. En sådan handling är i Försvarsmakten *sekretessklassificerad*. En handling som är märkt UNCLASSIFIED eller motsvarande är således inte att likställa med att den är offentlig. Det kan dock förekomma att en sådan handling är offentlig.

En handling från en annan stat eller en mellanfolklig organisation och som är märkt UNCLASSIFIED eller motsvarande kan även innehålla uppgifter som omfattas av andra sekretessbestämmelser i OSL, t.ex. sekretess för uppgifter om enskilds personliga eller ekonomiska förhållanden. Vid sekretessprövning av en handling som inkommer från en annan stat eller mellanfolklig organisation är det därför nödvändigt att inte enbart undersöka om ett röjande av uppgifterna stör Sveriges mellanfolkliga förbindelser.

9.1.6 Handlingar från EU som är märkta LIMITE

En handling som är märkt LIMITE lämnas ut internt inom Europeiska rådet, bland dess medlemmar, inom Europeiska kommissionen och vissa andra EU-institutioner och EU-organ. Sådana handlingar får överlämnas till alla tjänstemän vid medlemsstaternas nationella förvaltningar och Europeiska kommissionen.[112]

En handling som inkommer till Försvarsmakten från EU och som är märkt LIMITE kan i princip inte omfattas av försvarssekretess. Detta medför även att handlingen inte ska placeras i en informationssäkerhetsklass och ska därmed inte ges ett säkerhetsskydd. På grund av sin karaktär kan man anta att ett röjande av uppgifterna i handlingen stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet vilket medför att handlingen bör sekretessmarkeras med en hänvisning till 15 kap. 1 § OSL. I sådana fall är handlingen sekretessklassificerad i Försvarsmakten.

En handling enligt ovan kan även innehålla uppgifter som omfattas av andra sekretessbestämmelser i OSL, t.ex. sekretess för uppgifter om enskilds personliga eller ekonomiska förhållanden. Vid sekretessprövning av en handling som är märkt LIMITE är det därför nödvändigt att inte enbart undersöka om ett röjande av uppgifterna stör Sveriges mellanfolkliga förbindelser.

9.1.7 Handlingar från företag

Ett företag kan ha uppgifter som om de röjs till en konkurrent medför en skada för företaget. Företag omfattas inte av bestämmelserna i OSL varför de inte ska använda en sekretessmarkering. Ett företag kan uppmärksamma en myndighet på att en handling som skickas till myndigheten innehåller uppgifter som hos myndigheten omfattas av sekretess enligt OSL. Det finns ingen enhetlig definierad benämning när företag märker handlingar med avseende på uppgifter som behöver skyddas mot ett röjande. På sådana handlingar kan det därför förekomma en mängd olika benämningar, t.ex. FÖRETAGSHEMLIG. Det förekommer även att sådana handlingar är märkta med en uppmaning till myndigheten att handlingen ska sekretessmarkeras av myndigheten. Den vanligaste sekretessbestämmelsen i dessa sammanhang är 31 kap. 16 § OSL om sekretess för uppgift om en enskilds affärs- eller driftförhållande.

En handling som inkommer till Försvarsmakten från ett företag, med vilken Försvarsmakten har ingått en affärsförbindelse med, och som är märkt med en uppmaning till Försvarsmakten att handlingen ska sekretessmarkeras enligt 31 kap. 16 § OSL bör sekretessmarkeras då myndigheten normalt sätter tilltro till den bedömning som företaget har gjort. En sådan handling ska inte placeras i informationssäkerhetsklass då handlingen inte ska ges ett säkerhetsskydd.[113] En sådan handling är i Försvarsmakten

112 Europeiska unionens råd, informerande not 5847/06 Hantering av LIMITE-markerade handlingar.
113 Sidorna 24-25, Säkerhetsskydd prop. 1995/96:129.

sekretessklassificerad. I de fall handlingen även innehåller uppgifter som är hemliga eller utrikesklassificerade är handlingen hemlig respektive utrikesklassificerad och ska då placeras i informationssäkerhetsklass.

9.1.8 Felaktig användning av informationssäkerhetsklasserna

Försvarsmakten har definierat informationssäkerhetsklasserna i försvarsmaktens föreskrifter om säkerhetsskydd. Informationssäkerhetsklasserna är en indelning av säkerhetsskyddet i Försvarsmakten, samt i de myndigheter för vilka Försvarsmakten har föreskriftsrätt över. Syftet med informationssäkerhetsklasserna är att indela skyddet så att hemliga uppgifter som har en högre betydelse för bl.a. totalförsvaret ges ett högre skydd. På motsvarande sätt ges hemliga uppgifter som har en lägre betydelse ett lägre skydd. Då säkerhetsskydd inte avsett för uppgifter som inte rör rikets säkerhet[114] får inte sådana uppgifter placeras i informationssäkerhetsklass.

Vissa myndigheter använder informationssäkerhetsklasserna för handlingar utan att de rör rikets säkerhet eller ska ges ett motsvarande skydd enligt ett säkerhetsskyddsavtal med en annan stat eller mellanfolklig organisation. Konsekvenserna av att felaktigt placera uppgifter i informationssäkerhetsklass är ökade kostnader, risk för missförstånd vid informationsutbyte mellan myndigheter eller mellan Sverige och andra nationer eller mellanfolkliga organisationer.

Märkning om informationssäkerhetsklass ska överkorsas på en handling som inkommer till Försvarsmakten om avsändaren har sekretessmarkerat handlingen med en hänvisning till OSL som inte rör rikets säkerhet eller inte omfattas av sekretess enligt 15 kap. 1 § OSL (utrikessekretess) (exempel 9:1).

Exempel 9:1

En handling inkommer till Försvarsmakten från en annan myndighet. Handlingen har av myndigheten sekretessmarkerats med hänvisning till 31 kap. 16 § OSL och placerats i informationssäkerhetsklass HEMLIG/CONFIDENTIAL.

Märkningen med informationssäkerhetsklass ska på enklaste sätt överkorsas på handlingen. Handlingen är i Försvarsmakten sekretessklassificerad och ska sekretessmarkeras med en sådan sekretessmarkering med hänvisning till 31 kap. 16 § OSL.

9.1.9 Hemliga handlingar som inte är placerade i informationssäkerhetsklass

En inkommande *hemlig* handling som inte är placerad i informationssäkerhetsklass ska placeras i HEMLIG/SECRET om det inte är klart vilken annan informationssäker hetsklass som handlingen ska placeras i.[114]

En inkommande kvalificerat hemlig handling som inte är placerad i informationssäkerhetsklass ska placeras i HEMLIG/TOP SECRET.[114]

9.1.10 Otydlig sekretessmarkering

En handling som inkommer till Försvarsmakten och som har sekretessmarkerats av avsändaren men där hänvisning till bestämmelse i OSL saknas, alternativt är oläslig, får inte slentrianmässigt sekretessmarkeras med hänvisning till 15 kap. 2 § OSL eller placeras i informationssäkerhetsklass. Vid mottagande av en sådan handling bör upprättande myndighet, eller upprättande organisationsenhet i Försvarsmakten, kontaktas för att få klarhet i vilken bestämmelse i OSL som sekretessmarkeringen avser.

9.2 Upprättande av handlingar

Innan en handling skapas ska den person som skapar handlingen bedöma om handlingen kommer att innehålla någon uppgift som omfattas av sekretess enligt OSL. Om de sekretessbelagda uppgifterna rör rikets säkerhet eller är utrikesklassificerade ska personen också bedöma den högsta informationssäkerhetsklass som uppgifterna kommer att placeras i. Se avsnitt 6 om informationsklassificering.

Vilka märkningar som en handling ska ha beror på om handlingen är allmän eller inte (arbetshandling), om handlingen är hemlig, utrikesklassificerad eller sekretessklassificerad och i vilken eventuell informationssäkerhetsklass handlingen är placerad i.

En handling skapas normalt i ett IT-system. Endast ett IT-system som är ackrediterat, för det slag av uppgifter som handlingen bedöms komma att innehålla, får användas för att upprätta och vidare behandla handlingen (se kapitel 19 om ackreditering). CIO har dock möjlighet att fatta beslut om att IT-system som är avsedda för sekretessklassificerade uppgifter eller uppgifter som inte omfattas av sekretess inte behöver ackrediteras.

De märkningar som en handling ur säkerhetssynpunkt ska vara försedd med ska även finnas på en elektronisk handling och är inte begränsade till Microsoft Word utan även andra elektroniska format för handlingar, t.ex. Microsoft Excel (se även avsnitt 13.3 om portalparagrafen 7 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd).

114 Analogt med övergångsbestämmelsen 5 om äldre handlingar i Försvarsmaktens föreskrifter om säkerhetsskydd.

Även meddelandeblanketter inom Försvarsmaktens sambandstjänst, som kan förutsättas komma innehålla hemliga uppgifter när de används, ska utformas enligt de krav som gäller för märkning av hemliga handlingar.

9.2.1 Hemliga handlingar

En hemlig handling som är en allmän handling ska *sekretessmarkeras* (se avsnitt 9.5) och märkas med informationssäkerhetsklass på handlingens första sida. Om handlingen består av flera sidor ska det på sidan två och följande sidor finnas en hänvisning till informationssäkerhetsklassen på första sidan.

Syftet med sekretessmarkeringen är att varna personer som kommer i kontakt med handlingen att handlingen har bedömts innehålla någon uppgift som omfattas av sekretess enligt OSL. Märkningen om *informationssäkerhetsklass* på handlingen visar vilket säkerhetsskydd som den hemliga handlingen ska ges (se avsnitt 6.4).

I handlingen är det självklart att namnet på den myndighet som har upprättat handlingen ska anges. En lämplig placering är handlingens första sida.

9.2.2 Hemliga handlingar (H/C och högre)

Utöver sekretessmarkering och informationssäkerhetsklass ska en hemlig handling, som är en allmän handling och som är placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL, förses med märkningar för att uppnå *spårbarhet* i hanteringen av handlingen. Av märkningarna ska det också vara möjligt att se om handlingen är komplett.

I en allmän handling som är placerad i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre ska det på *sändlistan* till handlingen eller i det register där handlingen är diarieförd anges:

- hur många exemplar av handlingen som har framställts och

vilka som är mottagare av respektive exemplar.[115]

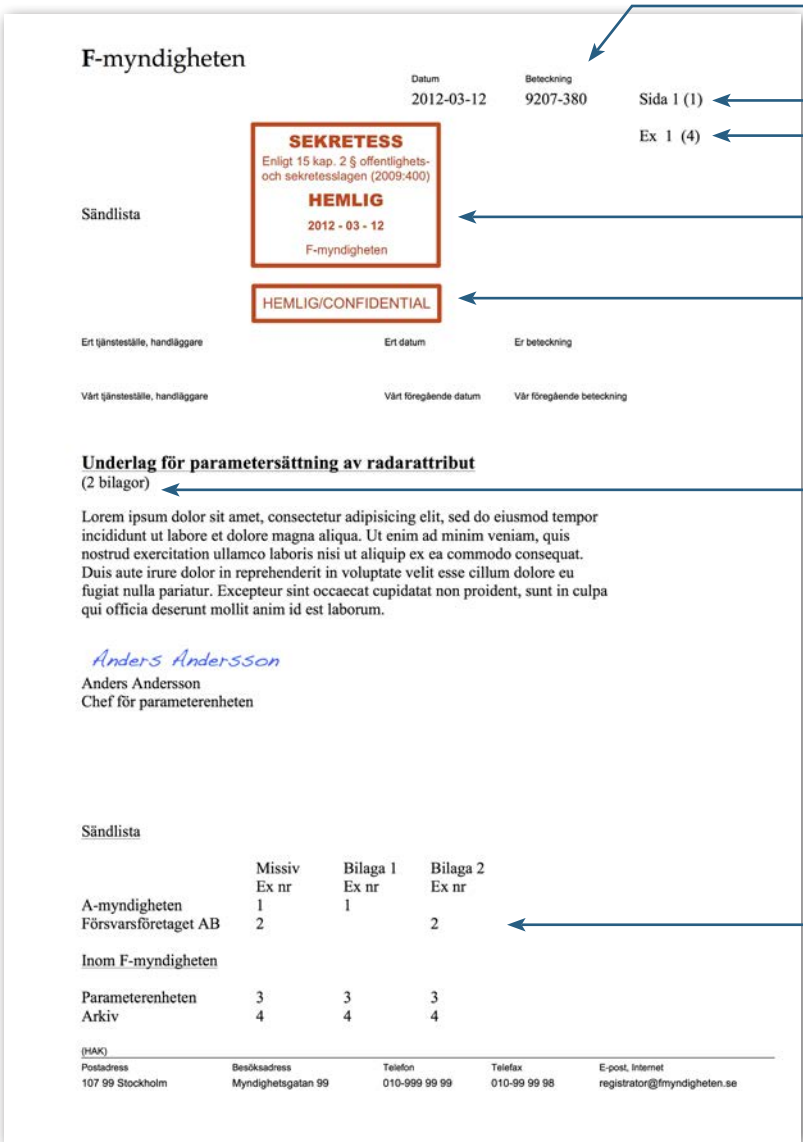
Vid framställning av en allmän handling som är hemlig och som är placerad i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högra ska på första sidan antecknas:

- handlingens beteckning,
- exemplarnummer,
- antal sidor samt
- antal bilagor, om sådana följer med.

115 2 kap. 7 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Sidorna ska numreras i följd. Av bilaga och blad i bok med lösbladssystem ska framgå till vilken handling bilagan respektive bladet hör.[116]

En hemlig handling som är en allmän handling och som är avsedd att användas gemensamt av flera personer (avsnitt 9.15) *får* sändlistan innehålla vilken grupp som är mottagare av handlingen.



F-myndigheten

Datum 2012-03-12 | Beteckning 9207-380 | Sida 1 (1)

Ex 1 (4)

SEKRETESS
Enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400)
HEMLIG
2012 - 03 - 12
F-myndigheten

Sändlista

HEMLIG/CONFIDENTIAL

Ert tjänsteställe, handläggare | Ert datum | Er beteckning

Vårt tjänsteställe, handläggare | Vårt föregående datum | Vår föregående beteckning

Underlag för parametersättning av radarattribut
(2 bilagor)

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Anders Andersson
Anders Andersson
Chef för parameterenheten

Sändlista

	Missiv Ex nr	Bilaga 1 Ex nr	Bilaga 2 Ex nr
A-myndigheten	1	1	
Försvarsföretaget AB	2		2
Inom F-myndigheten			
Parameterenheten	3	3	3
Arkiv	4	4	4

(HAK)

Postadress	Besöksadress	Telefon	Telefax	E-post, Internet
107 99 Stockholm	Myndighetsgatan 99	010-999 99 99	010-99 99 98	registrator@fmyndigheten.se

Beteckning eller diarienummer som tillsammans med exemplarnummer unikt identifierar handlingen.

Uppgift om *antal sidor*.

Uppgift om *antal exemplar*.

Sekretessmarkering (se avsnitt 9.5).

Informationssäkerhetsklass (se avsnitt 6.4).

Uppgift om *antal bilagor*.

Sändlista där det framgår hur *många exemplar* av handlingen som har framställts och *vilka som är mottagare* av respektive exemplar.

Bild 9:2 - Exempel på första sidan på en hemlig handling som är upprättad vid den fiktiva myndigheten F-myndigheten.

116 2 kap. 7 § Försvarsmaktens föreskrifter om säkerhetsskydd.

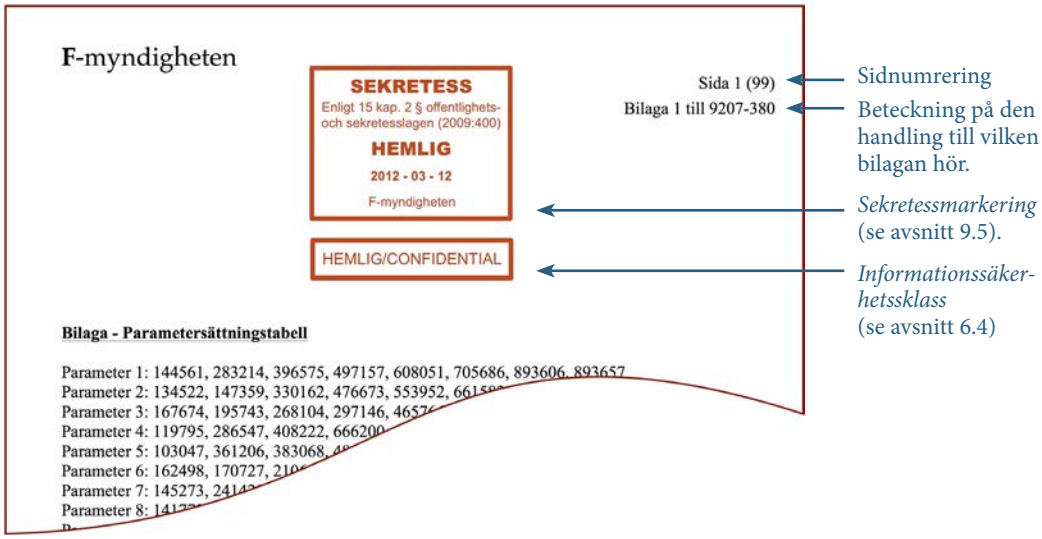


Bild 9:3 - Exempel på första sidan i en bilaga i en hemlig handling som är upprättad vid den fiktiva myndigheten F-myndigheten.

Bild 9:4 - Exempel på andra sidan i en bilaga i en hemlig handling som är upprättad vid den fiktiva myndigheten F-myndigheten.

9.2.3 Hemliga handlingar (H/R)

Även en hemlig handling som är en allmän handling och som är placerad i informationssäkerhetsklassen HEMLIG/RESTRICTED ska sekretessmarkeras och märkas med informationssäkerhetsklass på handlingens första sida. Om handlingen består av flera sidor ska det på sidan två och följande sidor finnas en hänvisning till informationssäkerhetsklassen på första sidan.

Krav på spårbarhet av varje exemplar eller att det ska vara möjligt att se om handlingen är komplett finns inte för en handling som är hemlig och som är placerad i informationssäkerhetsklassen HEMLIG/RESTRICTED. En sådan handling ska ur *säkerhetssynpunkt* därför inte förses med märkning om exemplarnummer, handlingens *beteckning*, *antal sidor* samt *antal bilagor*. Inte heller behöver den förses med en *sändlista* där det framgår vilka som är mottagare av varje exemplar. Sidorna i en sådan handling behöver inte vara numrerade.

För att skapa förutsättningar för ordning och reda i informationshanteringen får så klart en hemlig handling som är en allmän handling och som är placerad i informationssäkerhetsklassen HEMLIG/RESTRICTED förses med sändlista samt bilage- och sidnumrering. För att underlätta registrering av allmänna handlingar (se avsnitt 9.8) får[117] även en handling som är hemlig och som är en allmän handling och som är placerad i informationssäkerhetsklassen HEMLIG/RESTRICTED vara försedd med diarienummer eller liknande.

9.2.4 Utrikesklassificerade handlingar

En utrikesklassificerad handling ska i Försvarsmakten ges samma skydd som hemliga handlingar.[118] En utrikesklassificerad handling ska därför förses med de märkningar som en hemlig handling ska vara försedd med, t.ex. vad gäller exemplar- och sidnumrering.

9.2.5 Sekretessklassificerade handlingar

Ur säkerhetssynpunkt är det tillräckligt att en sekretessklassificerad handling som är en allmän handling enbart på första sidan är sekretessmarkerad. Någon hänvisning till första sidan behöver inte finnas på sidan två och följande sidor i handlingen. Dokumentmallar ska därför inte innehålla någon sådan hänvisning. Se avsnitt 9.5.4 om sekretessmarkering av en sekretessklassificerad handling som är en allmän handling.

Krav på spårbarhet av varje exemplar eller att det ska vara möjligt att se om handlingen är komplett finns i Försvarsmakten inte för en sekretessklassificerad handling.

En sekretessklassificerad handling ska inte placeras i informationssäkerhetsklass eller förses med märkningar om exemplarnummer. Ur *säkerhetssynpunkt* ska den inte förses med märkning om exemplarnummer, handlingens *beteckning*, *antal sidor* samt *antal bilagor*. Inte heller behöver den förses med en *sändlista* där det framgår vilka som är mottagare av varje exemplar. Sidorna i en sådan handling behöver ur säkerhetssynpunkt inte vara numrerade. För att skapa förutsättningar för ordning och reda

117 Sidan 358, Förslag till sekretesslag m.m. prop. 1979/80:2 Del A.

118 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

i informationshanteringen får så klart en sekretessklassificerad handling förses med sändlista samt bilage- och sidnumrering. För att underlätta registrering av allmänna handlingar (se avsnitt 9.8) får[119] även en sekretessklassificerad handling vara försedd med diarienummer eller liknande.

9.2.6 Beskrivning av sekretessbedömning i en handling

En mottagare av en sekretessmarkerad handling har inte alltid kunskap om *vilka* uppgifter i handlingen som omfattas av sekretess enligt OSL. För att underlätta vidare sekretessbedömning av en sekretessmarkerad handling får handlingen förses med en beskrivning av vilka uppgifter i handlingen som omfattas av sekretess och vilka sekretessbestämmelser i OSL som har bedömts gälla för uppgifterna. En sådan beskrivning kan placeras i handlingens inledande avsnitt eller i handlingens missiv (exempel 9:2 och exempel 9:3).

Exempel 9:2

Avsnitt 7.4 i handlingen innehåller uppgifter om vapenkassuners konstruktion och skyddsegenskaper. Uppgifterna bedöms omfattas av sekretess enligt 18 kap. 8 § offentlighets- och sekretesslagen (2009:400). Uppgifterna är i Försvarsmakten sekretessklassificerade.

Exempel 9:3

Bilaga 21 innehåller uppgifter om teleförbindelser till fasta grupperingsplatser i Stockholms skärgård. Uppgifterna bedöms omfattas av sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400) och vara placerade i informationssäkerhetsklass HEMLIG/SECRET.

9.3 Märkning av handlingar i internationella samarbeten

I ett internationellt samarbete kan det finnas bestämmelser för det specifika samarbetet, eller bestämmelser i säkerhetsskyddsavtal med en annan stat, som innebär att handlingar i samarbetet även ska förses med särskilda märkningar. T.ex. ska handlingar som ska överföras till Estland där så är möjligt även förses med den estländska motsvarigheten till informationssäkerhetsklass.[120] Innan ett internationellt samarbete

119 Sidan 358, Förslag till sekretesslag m.m. prop. 1979/80:2 Del A.
120 Artikel 1 i Avtal med Estland om skydd av sekretessbelagd information (SÖ 2002:10).

påbörjas är det därför av betydelse att undersöka om det finns några bestämmelser som är tillämpliga på handlingar i ett sådant samarbete.

> *Hemliga handlingar som sänds utomlands skall förses med anteckning om uppgifternas ursprungsland.*
>
> 2 kap. 25 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

I enlighet med vad som är internationellt vedertaget ska svenska hemliga handlingar som delges till utländska myndigheter förses med en anteckning om att ursprunget är svenskt. Denna anteckning kan även medföra särskilda krav på hantering hos mottagaren som t.ex. att vidare spridning inte får ske. Sådana bestämmelser kan framgå av bi- eller multilaterala säkerhetsskyddsavtal eller i projektsäkerhetsinstruktioner för det aktuella samarbetet.

En myndighets anteckning kan utformas genom märkningen *Country of origin: Sweden* som påförs en handling. Då det av en sekretessmarkering i Försvarsmakten även ska framgå myndighetens namn på engelska behöver en sekretessmarkerad handling som ska sändas utomlands inte förses med någon särskild anteckning om uppgifternas ursprungsland.

9.4 Märkning av handlingar i utbildning och övning

Under utbildning och övning kan det finnas ett behov av att hantera handlingar på samma sätt som *om* de hade innehållit uppgifter som omfattas av sekretess enligt OSL, även om handlingarna *inte* innehåller någon sådan uppgift. För att personalen ska få erfarenhet av att hantera handlingarna behöver handlingarna märkas med t.ex. sekretessmarkering och informationssäkerhetsklass.

En handling som uteslutande används under utbildning och övning och som inte innehåller någon uppgift som omfattas av sekretess får märkas med sekretessmarkering, informationssäkerhetsklass m.fl. märkningar om handlingens alla sidor innehåller anteckningen *UTBILDNING – EJ SEKRETESS*. Anteckningen ska vara tydligt angiven så att det är uppenbart för en person som ser handlingen att det är fråga om en handling som används i utbildningssyfte. En sådan handling får då endast hanteras inom en avgränsad verksamhet, t.ex. under utbildning av sambandspersonal. En sådan handling ska förstöras efter utbildningen om det enligt arkivlagstiftningen finns stöd för förstöringen. Om handlingen inte får förstöras ska sekretessmarkeringen och informationssäkerhetsklass överkorsas.

I internationella samarbeten är det lämpligt att före en övning överenskomma om hur handlingar som används under utbildning och övning ska märkas (kapitel 4).

Även om det under utbildning eller övning förekommer fiktiva uppgifter som i sig inte omfattas av sekretess enligt OSL kan uppgifterna röja t.ex. metoder, analyskapacitet etc. som bedömts omfattas av sekretess enligt OSL. I sådana fall ska uppgifterna sekretessbedömas och hanteras enligt det regelverk som gäller för de aktuella uppgifternas informationsklassificering. Handlingar som innehåller sådana uppgifter får inte förses med anteckningen *UTBILDNING – EJ SEKRETESS*.

Under en övning kan även handlingar som innehåller uppgifter som omfattas av sekretess komma att användas, t.ex. Försvarsmaktens beredskaps- och insatsorder. Sådana handlingar får inte förses med anteckningen *UTBILDNING – EJ SEKRETESS*. Handlingarna ska hanteras enligt det regelverk som gäller för de aktuella uppgifternas informationsklassificering.

9.5 Sekretessmarkering

En handling får endast sekretessmarkeras om den innehåller någon uppgift som omfattas av sekretess enligt OSL.[121] De uppgifter i handlingen som bedöms omfattas av sekretess ska antas uppfylla de villkor (rekvisit) som anges i de sekretessbestämmelser som sekretessmarkeringen hänvisar till.

I OSL är bestämmelsen om sekretessmarkering (tidigare hemligstämpel) teknikneutral. Även handlingar som är elektroniska ska förses med sekretessmarkering alternativt att sekretessmarkering anges i det IT-system där en sådan handling hanteras. Det är upp till en myndighet att avgöra vad en sekretessmarkering ska innehålla förutom de obligatoriska uppgifter som anges i 5 kap. 5 § OSL. Sekretessmarkeringar kan därför ha olika utseende hos olika myndigheter. Beteckningen hemlig behöver inte ingå i en sekretessmarkering.

121 2 kap. 16 § TF.

Om det kan antas att en uppgift i en allmän handling inte får lämnas ut på grund av en bestämmelse om sekretess, får myndigheten markera detta genom att en särskild anteckning (sekretessmarkering) görs på handlingen eller, om handlingen är elektronisk, införs i handlingen eller i det datasystem där den elektroniska handlingen hanteras. Anteckningen ska ange

1. tillämplig sekretessbestämmelse,

2. datum då anteckningen gjordes, och

3. den myndighet som har gjort anteckningen.

Om utlämnande till en enskild av en uppgift i en allmän handling som är av synnerlig betydelse för rikets säkerhet enligt förordning ska prövas endast av en viss myndighet, ska en sekretessmarkering göras så snart som möjligt. Av anteckningen ska det framgå vilken myndighet som ska pröva frågan om utlämnande.

5 kap. 5 § OSL

Att beteckningen hemlig ingår i en sekretessmarkering behöver inte innebära att de sekretessbelagda uppgifterna rör rikets säkerhet. I 1980 års sekretesslag uppställdes krav på att en hemligstämpel skulle innehålla beteckningen hemlig, oavsett vilken sekretessbestämmelse som sekretessen avsåg och oavsett om uppgifter rörde rikets säkerhet. Användningen av beteckningen hemlig kolliderade därför med definitionen av begreppet hemlig uppgift i 4 § säkerhetsskyddsförordningen där hemlig enbart avser uppgifter som rör rikets säkerhet.

En myndighet behöver generellt inte sekretessmarkera alla handlingar som innehåller en uppgift som omfattas av sekretess. För handlingar som är av synnerlig betydelse för rikets säkerhet (kvalificerat hemliga) finns dock ett ovillkorligt krav i 5 kap. 5 § OSL på att en sådan handling alltid ska sekretessmarkeras. Med hänsyn till uppgifters betydelse och om avsaknaden av en sekretessmarkering kan orsaka att uppgifterna röjs kan det vara nödvändigt att även andra slag av handlingar sekretessmarkeras. T.ex. ska handlingar som innehåller hemliga uppgifter sekretessmarkeras hos de myndigheter som Försvarsmakten och Rikspolisstyrelsen har föreskriftsrätt över vad gäller säkerhetsskydd.

Allmänna handlingar som innehåller någon uppgift som omfattas av sekretess enligt OSL ska sekretessmarkeras i Försvarsmakten.[122] [123] [124] Om en allmän handling inne-

122 2 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd.

123 2 kap. 3 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

124 3 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

håller en kombination av uppgifter som bedöms omfattas av sekretess enligt olika bestämmelser i OSL ska handlingen minst märkas med den sekretessmarkering som ger det högsta skyddet. Flera sekretessmarkeringar får i sådana fall också användas. I Försvarsmakten anges myndigheten Försvarsmakten, på svenska och engelska, och inte namn på organisationsenhet eller förband. Genom att myndighetens namn anges på engelska behöver inte en hemlig eller utrikesklassificerad handling som ska sändas utomlands förses med ytterligare en anteckning om uppgifternas ursprungsland.[125]

En sekretessmarkering är enbart en varningssignal om att det kan finnas uppgifter i en handling som bedöms vara sekretessbelagda enligt OSL. Att sekretessmarkera en handling innebär inte något bindande avgörande av sekretessfrågan. Innan en handling lämnas ut ska därför en sekretessprövning av innehållet göras oavsett om handlingen är försedd med sekretessmarkering eller inte. En sekretessprövning ska göras i varje enskilt fall och grundas på de uppgifter som förekommer i handlingen.

En sekretessprövning avser inte enbart om en handling innehåller hemliga uppgifter. Om enbart förekomsten av hemliga uppgifter skulle uppmärksammas i en sekretessprövning kan det innebära att *utrikesklassificerade* och *sekretessklassificerade* uppgifter röjs och därmed skadar de intressen som sekretessbestämmelserna i det enskilda fallet ska skydda. Det är därför nödvändigt att under en sekretessprövning uppmärksamma förekomsten av såväl *hemliga* som *utrikesklassificerade* som *sekretessklassificerade* uppgifter. Det är viktigt att understryka att sekretessprövning ska göras oberoende av om handlingen är sekretessmarkerad eller inte. Det är således inte tillåtet att vägra att lämna ut en handling enbart med hänvisning till att den är sekretessmarkerad.

9.5.1 Sekretessmarkering i IT-system

Informationstillgångar behandlas i mycket stor omfattning i IT-system. Behovet av den varningssignal som sekretessmarkeringen utgör är lika stort för elektroniska handlingar som för handlingar av papper. Elektroniska handlingar är inte begränsade till dokument som utgör en direkt motsvarighet till pappersdokument (t.ex. en PDF-fil). Elektroniska handlingar avser även skärmbilder där uppgifter presenteras (t.ex. av poster i en databas). Även e-post och andra upptagningar i IT-system utgör elektroniska handlingar.

I de fall det inte är möjligt att införa en sekretessmarkering i en elektronisk handling ska sekretessmarkeringen istället införas i det IT-system där den elektroniska handlingen hanteras. Hur detta anordnas är beroende av vilka funktioner som finns i IT-systemet och vad som är möjligt att åstadkomma. En sådan sekretessmarkering får utformas på lämpligt sätt – det väsentliga är att innebörden av uppgifterna i sekretessmarkeringen framgår enligt 5 kap. 5 § OSL. Sekretessmarkeringen kan utformas så att det i skärmbilden framgår vilka uppgifter eller handlingar som är sekretessmar-

125 2 kap. 25 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd.

kerade och eventuell placering i informationssäkerhetsklass. Det kan vara lämpligt att använda förkortningar (bild 9:5).

Om en hemlig handling skrivs ut från ett IT-system och handlingen har en tydligt läsbar sekretessmarkering på första sidan behöver inte pappershandlingen sekretessmarkeras på nytt med en gummistämpel.

Om sekretessmarkering ska införas i ett filnamn bör markeringen och informationssäkerhetsklass anges på ett för IT-systemet enhetligt sätt (bild 9:6 visar ett exempel). I IT-system kan det vara lämpligt att använda förkortningarna H/TS, H/S, H/C och H/R för informationssäkerhetsklasserna.

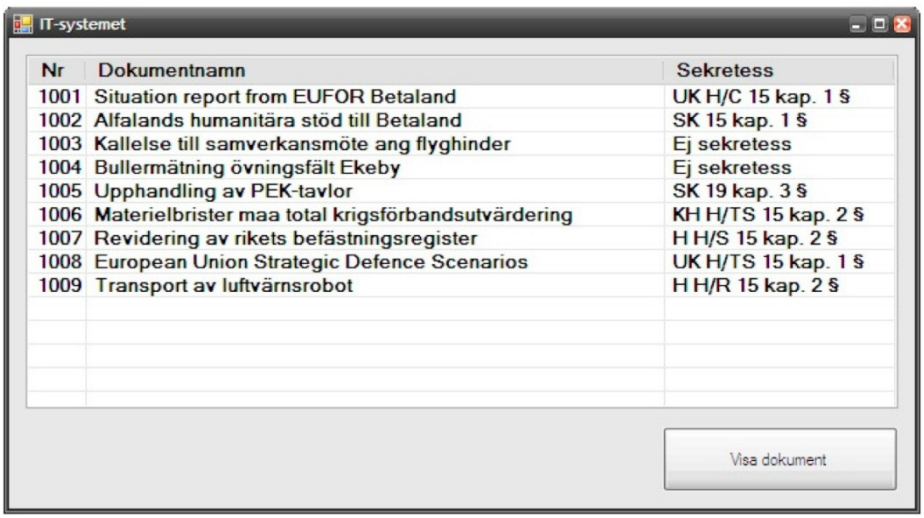


Bild 9:5 - Exempel på hur sekretessmarkering skulle kunna införas i ett IT-system där elektroniska handlingar hanteras och det inte är möjligt att införa sekretessmarkeringen i den elektroniska handlingen.

```
G:\katalog\Situation report (HEMLIG 15.2 2012-05-14
Försvarsmakten HS).doc
```

Bild 9:6 - Exempel på sekretessmarkering (parentesen) i ett filnamn för en elektronisk handling.

9.5.2 Sekretessmarkering för hemliga handlingar som är allmänna handlingar

För sekretessmarkering i Försvarsmakten som avser allmänna handlingar som innehåller någon hemlig uppgift ska beteckningen HEMLIG även fortsättningsvis ingå i sekretessmarkering. Begreppet HEMLIG på sådana handlingar korresponderar mot begreppen hemlig uppgift och hemlig handling som är definierade i 4 § säkerhets-

skyddsförordningen. Dessutom finns beteckningen angiven i flera av Sveriges säkerhetsskyddsavtal med andra stater.

En handling som innehåller såväl *hemliga* som *utrikesklassificerade* uppgifter ska minst märkas med den sekretessmarkering som ger det högsta skyddet, d.v.s. HEMLIG. I sekretessmarkeringarna får hänvisning göras till alla relevanta sekretessbestämmelser som hör till respektive sekretessmarkering.

9.5.3 Sekretessmarkering för utrikesklassificerade handlingar som är allmänna handlingar

En allmän handling som är utrikesklassificerad ska på första sidan förses med en särskild anteckning (sekretessmarkering) om att den är utrikesklassificerad. I fråga om en elektronisk handling ska sekretessmarkeringen i stället införas i handlingen eller i det IT-system där den elektroniska handlingen hanteras. Bestämmelser om sekretessmarkering finns i 5 kap. 5 § offentlighets- och sekretesslagen (2009:400).

Sekretessmarkeringen på den allmänna handlingen ska ha en enkel rektangulär ram.

2 kap. 3 § första och andra styckena Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Indelningen av Försvarsmaktens informationstillgångar ifråga om sekretess i hemliga, utrikesklassificerade samt sekretessklassificerade uppgifter medför även att informationstillgångarna behöver förses med motsvarande märkning. Bestämmelsen innebär att utrikesklassificerade allmänna handlingar ska sekretessmarkeras och att det i sekretessmarkeringen ska framgå att handlingen är utrikesklassificerad. En utrikesklassificerad handling som inte är allmän ska på första sidan förses med anteckning om att den är utrikesklassificerad. Ifråga om en elektronisk handling är det lämpligt att beteckningen UTRIKESKLASSIFICERAD anges på första sidan för denna anteckning. Ifråga om handlingar som förs för hand är det lämpligt att använda förkortningen UK för denna anteckning.

9.5.4 Sekretessmarkering för sekretessklassificerade handlingar

En allmän handling som är sekretessklassificerad ska på första sidan förses med en särskild anteckning (sekretessmarkering) om att handlingen är sekretessklassificerad. I fråga om en elektronisk handling ska sekretessmarkeringen i stället införas i handlingen eller i det IT-system där den elektroniska handlingen hanteras. Bestämmelser om sekretessmarkering finns i 5 kap. 5 § offentlighets- och sekretesslagen (2009:400).

En sekretessmarkering på en allmän handling ska ha en enkel rektangulär ram.

3 kap. 1 § första och andra styckena Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

En sekretessklassificerad handling behöver inte sekretessmarkeras om den ingår i en ordnad samling av handlingar som rör likartad verksamhet och som förvaras skyddad.

3 kap. 2 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Med en ordnad samling av handlingar som rör likartad verksamhet avses handlingar som hanteras avgränsat inom en verksamhet och som är ordnade så att handlingarna går att hänföra till det som handlingarna i huvudsak avser som t.ex. medicinska journaler och personalakter.

Föreskriften ska tolkas restriktivt i fråga om vad som utgör likartad verksamhet. Huvudregeln är att sekretessklassificerade handlingar ska sekretessmarkeras.

Med att handlingarna förvaras skyddade avses att det enbart är den personal som hanterar handlingarna i verksamheten som har åtkomst till handlingarna (t.ex. den personal som hanterar medicinska journaler och den personaladministrativa personalen som hanterar personalakter). Normalt har den personal som hanterar sådana handlingar kunskap om de sekretessbestämmelser som är tillämpliga för uppgifterna i verksamheten, varför behovet av sekretessmarkering inte är lika stort som i annan verksamhet.

En sekretessklassificerad allmän handling som enligt bestämmelsen inte behöver sekretessmarkeras ska dock sekretessmarkeras om handlingen inte längre ingår i en ordnad samling av handlingar som rör likartad verksamhet. En sekretessklassificerad

allmän handling som t.ex. ingår i en personalakt och som tas ut ur personalakten för att hanteras i en annan verksamhet ska sekretessmarkeras.

Föreskriften är även tillämplig i fråga om sekretessmarkering på elektroniska handlingar. För att elektroniska handlingar i ett IT-system inte ska behöva sekretessmarkeras krävs att IT- systemet är avsett för den avgränsade verksamheten där de elektroniska handlingarna hanteras (t.ex. ett IT-system för patientjournaler eller personalakter).

Med hänsyn till det stora antalet användare i Försvarsmaktens generella kontorsadministrativa IT-system (t.ex. FM AP och FMG) ska sekretessklassificerade handlingar normalt sekretessmarkeras när de hanteras i sådana IT-system.

9.5.5 Sekretessmarkeringens utseende

Bild 9:7 *- Sekretessmarkering i Försvarsmakten för en kvalificerat hemlig handling.*

Bild 9:8 *- Sekretessmarkering i Försvarsmakten för en hemlig handling som inte är av synnerlig betydelse för rikets säkerhet.*

Bild 9:9 *- Sekretessmarkering i Försvarsmakten för en utrikesklassificerad handling.*

Bild 9:10 *- Sekretessmarkering i Försvarsmakten för en sekretessklassificerad handling.*

En sekretessmarkering för en hemlig handling som är en allmän handling ska ha en rektangulär ram. Ramen ska vara enkel för en hemlig handling och dubbel för en kvalificerat hemlig handling.[126] I en sekretessmarkering för en kvalificerat hemlig handling ska det även framgå vilken myndighet som ska pröva frågan om utlämnande.[127] Sekretessmarkeringen bör vara röd. Uppgifter i en sekretessmarkering (t.ex. tillämplig sekretessbestämmelse) får antecknas för hand.

I en sekretessmarkering i Försvarsmakten ska sekretesskategorin (kvalificerat hemlig, hemlig, utrikesklassificerad eller sekretessklassificerad) anges. MUST har beslutat hur sekretessmarkeringar ska vara utformade i Försvarsmakten [referens 24] (exempel i bild 9:7, bild 9:8, bild 9:9 och bild 9:10). På grund av tekniska skäl kan gummistämplar vara utformade så att datum och sekretesskategorin byter plats.

9.5.6 Överkorsning av sekretessmarkering

Den bedömning avseende sekretess enligt OSL som har gjorts då en handling har inkommit eller upprättats kan ändras i efterhand. En sådan ändring kan vara aktuell oavsett om handlingen är kvalificerat hemlig, hemlig, utrikesklassificerad eller sekretessklassificerad. Det finns inte någon föreskrift om att allmänna handlingar som är sekretessmarkerade ska sekretessprövas med en viss regelbundenhet. Istället får en sådan prövning ske vid behov, t.ex. vid begäran om utlämnande av allmän handling eller om det av något annat skäl behöver prövas. Stöd för den som ska pröva frågan om utlämnande av en allmän handling finns i H Säk Sekrbed A.

Grunden för att få överkorsa en sekretessmarkering är att handlingen inte längre bedöms innehålla någon uppgift som omfattas av sekretess enligt OSL. *Huvudregeln inom svensk rätt är att den myndighet som har uppgiften också ska hantera och pröva de sekretessfrågor som kan uppstå kring uppgiften.* Från denna huvudregel finns endast två undantag:

1. En begäran att få ta del av en handling som omfattas av sekretess enligt 15 kap. 2 § OSL och som har upprättats av den *statliga lantmäterimyndigheten* eller *Sjöfartsverket* och som innehåller *kart- eller flygbildmaterial av betydelse för totalförsvaret* eller uppgift ur myndighetens *geodetiska arkiv* ska prövas av den myndighet som har upprättat handlingen.[128]

2. En begäran om utlämnande till en enskild av en allmän handling som är *kvalificerat hemlig* endast får prövas av myndigheter som anges i 1 § OSF.

126 2 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd.
127 5 kap. 5 § OSL.
128 15 kap. 4 § OSL.

I många länder tillämpas en princip som på engelska brukar kallas ”originator control.” Denna princip innebär att den som har upprättat en handling äger rätten att styra till vem handlingen lämnas även efter att den har överlämnats till exempelvis andra myndigheter eller andra stater.[129] Principen brukar även användas för upprättarens rättighet att styra ändringar av en handlings ursprungliga informationsklassificering. Någon generell rättslig reglering som motsvarar ”originator control” saknas i Sverige (se även avsnitt 7.8 om begränsning i att delge eller använda en handling). Utöver de två ovan beskrivna undantagen gäller således att frågan om uppgifterna i en handling fortsatt omfattas av sekretess prövas självständigt inom en myndighet, eller i Försvarsmakten inom en organisationsenhet, där handlingen förvaras.

För att kunna bedöma om en sekretessmarkerad handling fortsatt innehåller någon uppgift som omfattas av sekretess enligt OSL behöver den som utför prövningen kunskap om det ämne som uppgifterna rör. Om sådan kunskap inte finns och handlingen har upprättats vid en annan myndighet, eller i Försvarsmakten vid en annan organisationsenhet, är det lämpligt att samverkan sker med den andra myndigheten eller organisationsenheten. Även om en sådan samverkan sker är det fortfarande den myndighet, eller organisationsenhet i Försvarsmakten, som förvarar handlingen som självständigt prövar frågan om sekretess. Den myndighet, eller organisationsenhet i Försvarsmakten, som samverkan sker med kan inte avgöra frågan utan endast uttrycka sin uppfattning, t.ex. vilka uppgifter som bedöms omfattas av sekretess enligt OSL. Om bedömningen avser en *kvalificerat hemlig* handling ska samverkan alltid ske.[130]

För att undvika ett offentliggörande av en uppgift som kan störa Sveriges mellanfolkliga förbindelser bör den som avser att överkorsa en sekretessmarkering på en *utrikesklassificerad* handling ha kunskap om de berörda staternas och mellanfolkliga organisationernas syn på sekretess. I H Säk Sekrbed A beskrivs bl.a. utrikessekretessen.

För hemliga handlingar finns det föreskrifter om hur en sekretessmarkering ska överkorsas och åtgärder i samband med överkorsning.

129 Sidorna 193-194, Insyn och sekretess – i statliga företag – i internationellt samarbete (SOU 2004:75).
130 2 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Om en handling som är försedd med hemligstämpel inte längre bedöms vara hemlig skall beslut om detta antecknas på handlingen. Anteckningen skall innehålla myndighetens namn, datum för beslutet samt vem som har fattat beslutet. Därefter skall hemligstämpeln överkorsas och anteckning om beslutet göras i det register där handlingen är diarieförd.

2 kap. 4 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Sekretessmarkeringen och eventuell informationssäkerhetsklass överkorsas (se exempel i bild 9:11). Beslutet om överkorsning antecknas i det register där handlingen är diarieförd.[131] Om handlingen består av flera sidor är det lämpligt att på alla sidor överkorsa hänvisningen till sekretessmarkeringen på första sidan. Det är lämpligt att det av arbetsordning eller motsvarande framgår vem vid en myndighet som får fatta beslutet.

Bild 9:11 - Exempel på överkorsning av sekretessmarkering.

131 2 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Föreskriftens första stycke gäller även för en *utrikesklassificerad* handling.[132] Någon motsvarande föreskrift för *sekretessklassificerade* handlingar saknas. Om en sekretessklassificerad handling överkorsas behöver inte en anteckning om beslutet anges på handlingen.

> *Om en handling, som har försetts med den hemligstämpel som gäller för en kvalificerat hemlig handling, inte längre bedöms som kvalificerat hemlig skall samråd ske med den som har upprättat handlingen innan åtgärder vidtas enligt första stycket. Anteckning om samrådet skall göras på handlingen.*
>
> 2 kap. 4 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Samrådet sker då med den som har upprättat handlingen, t.ex. en annan myndighet eller organisationsenhet i Försvarsmakten. Om handlingen inte längre bedöms vara kvalificerat hemlig men fortfarande innehålla uppgifter som är hemliga ska handlingen sekretessmarkeras med en ny sekretessmarkering.

Föreskriftens andra stycke gäller inte för en *utrikesklassificerad* handling.[133] Någon motsvarande föreskrift för *sekretessklassificerade* handlingar saknas.

> *Om en handling som är försedd med anteckning som avses i 1 § tredje stycket i detta kapitel inte längre bedöms vara hemlig, skall anteckningen överkorsas. På handlingen skall vidare anges vem som har beslutat överkorsningen.*
>
> 2 kap. 4 § tredje stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Tredje stycket rör handlingar som inte är allmänna handlingar (arbetshandlingar). I avsnitt 9.7 beskrivs märkning av arbetshandlingar.

Föreskriftens tredje stycke gäller även för en *utrikesklassificerad* handling.[134] Någon motsvarande föreskrift för *sekretessklassificerade* handlingar saknas. På en sekretessklassificerad handling behöver inte anges vem som har beslutat överkorsningen.

---

132 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

133 2 kap. 1 § 1 b Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

134 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Om det vid en organisationsenhet bedöms att en allmän hemligstämplad handling, som har upprättats vid någon annan organisationsenhet eller en annan myndighet, inte längre är hemlig, ska den organisationsenhet respektive den myndighet som har upprättat handlingen underrättas.

2 kap. 1 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Det kan även rekommenderas att de organisationsenheter och myndigheter som finns med på sändlistan i den hemliga handlingen informeras om att handlingen inte längre bedöms innehålla några hemliga uppgifter. Även om handlingen inte längre bedöms innehålla några hemliga uppgifter kan handlingen fortfarande innehålla andra uppgifter som omfattas av sekretess enligt OSL men som inte rör rikets säkerhet. Om handlingen bedöms innehålla sådana uppgifter är det lämpligt att detta framgår av informationen till de andra myndigheterna och organisationsenheterna.

Föreskriften gäller även för en *utrikesklassificerad* handling.[135] Någon motsvarande föreskrift för *sekretessklassificerade* handlingar saknas. Om en sekretessklassificerad handling har upprättats vid en annan myndighet, eller en annan organisationsenhet, behöver inte den andra myndigheten, eller organisationsenheten, underrättas om överkorsningen.

9.5.7 Överkorsning av sekretessmarkering i IT-system

Grunderna för överkorsning beskrivs i avsnitt 9.5.6. Hur överkorsning av sekretessmarkering ska anordnas i ett IT-system är beroende av vilka funktioner som finns i IT-systemet och vad som är möjligt att åstadkomma. När ett IT-system utvecklas är det nödvändigt att uppmärksamma behovet av tekniska funktioner som gör det möjligt att överkorsa sekretessmarkering i en elektronisk handling (avsnitt 13.3). I ett IT-system som innehåller elektroniska handlingar i form av dokumentfiler är det lämpligt att överkorsning av en sekretessmarkering sker i handlingens dokumentfil. T.ex. är det möjligt att ändra ett PDF-dokument om dokumentets skyddsinställningar tillåter ändringar.

I de fall ett PDF-dokument inte går att ändra och det ursprungliga dokumentet är tillgängligt bör ett nytt PDF-dokument skapas där sekretessmarkeringen har överkorsats. Om det ursprungliga dokumentet inte är tillgängligt bör PDF-dokumentet skrivas ut på papper, överkorsningen genomföras och pappersdokumentet därefter skannas in.

135 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Versionshantering, t.ex. i ett dokument- och ärendehanteringssystem, underlättar överkorsning av en sekretessmarkering i en elektronisk handling. Om det i ett IT-system finns ett register över handlingarna och det av registret framgår handlingarnas informationsklassificering måste överkorsningen av en handlings sekretessmarkering även framgå i registret.

9.6 Märkning av informationssäkerhetsklass på en allmän handling

En hemlig handling skall placeras i en av de informationssäkerhetsklasser som anges i 1 kap. 4 §. Handlingen skall på första sidan förses med en uppgift om i vilken informationssäkerhetsklass den har placerats.

2 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

På en allmän handling som är kvalificerat hemlig, hemlig eller utrikesklassificerad anges informationssäkerhetsklassen på handlingens första sida. Märkningen ska vara tydlig och bör vara röd. En lämplig placering är under sekretessmarkeringen (exempel i bild 9:12). Märkning med informationssäkerhetsklass kan även anges i handlingens sidhuvud.

En handling som är sekretessklassificerad ska inte placeras i informationssäkerhetsklass och får därför inte förses med en informationssäkerhetsklass.

Bild 9:12 - *Exempel på märkning med informationssäkerhetsklass under en sekretessmarkering.*

På en handling som innehåller uppgifter som är placerade i olika informationssäkerhetsklasser är det den högsta informationssäkerhetsklassen, som någon av uppgifterna är placerade i, som ska anges på handlingens första sida (exempel 9:4).

Exempel 9:4

En allmän handling innehåller *hemliga* uppgifter som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL och *utrikesklassificerade* uppgifter som är placerade i informationssäkerhetsklass HEMLIG/SECRET.

Handlingens första sida ska minst sekretessmarkeras med sekretessmarkeringen för HEMLIG handling. Handlingens första sida ska märkas med informationssäkerhetsklassen HEMLIG/SECRET.

Om en hemlig handling består av flera sidor skall på varje sida finnas en hänvisning till uppgiften om informationssäkerhetsklass på första sidan.

2 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd

Hänvisningen får även innehålla vilken informationssäkerhetsklass som handlingen är placerad i.

Se även avsnitt 9.5.1 om märkning med informationssäkerhetsklass i IT-system.

9.6.1 Ändring av informationssäkerhetsklass

Om en handling placeras i en annan informationssäkerhetsklass än vad som anges på handlingen ska detta antecknas på handlingen. En sådan anteckning ska innehålla

- den nya informationssäkerhetsklassen,
- myndighetens namn,
- datum för beslutet samt
- vem som fattat beslutet.[136]

136 2 kap. 5 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Bild 9:13 *- Exempel på anteckning om ändrad informationssäkerhetsklass på en hemlig handling.*

Den tidigare angivna informationssäkerhetsklassen överkorsas. Den nya informationssäkerhetsklassen anges i anslutning till den tidigare angivna informationssäkerhetsklassen (bild 9:13).

Om handlingen är allmän ska beslutet om ändring av informationssäkerhetsklass föras in i det register där handlingen är registrerad. En ändring av informationssäkerhetsklass kan bl.a. resultera i nya kvitterings- och inventeringsrutiner för aktuell handling.

Den organisationsenhet som gör bedömningen att en allmän handling som är hemlig ska placeras i en annan informationssäkerhetsklass än den ursprungliga ska underrätta den organisationsenhet eller myndighet som har upprättat handlingen.[137] Det är lämpligt att de organisationsenheter och myndigheter som finns med på sändlistan i den hemliga handlingen informeras om att handlingen placeras i en annan informationssäkerhetsklass.

9.6.2 Överkorsning av informationssäkerhetsklass

Om en handling inte längre ska vara placerad i informationssäkerhetsklass ska anteckningen om informationssäkerhetsklass överkorsas.[138] På handlingen ska anges vem som har beslutat om överkorsningen (bild 9:14).

137 2 kap. 1 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
138 2 kap. 5 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Handlingen är inte hemlig
2013-04-09
Försvarsmakten, F 17

Carls Carlsson
Övlt Carl Carlsson

Bild 9:14 - Exempel på beslut om överkorsning av informationssäkerhetsklass på en handling som inte är en allmän handling.

9.7 Märkning av arbetshandlingar

Med *arbetshandling* avses här en handling som inte är en allmän handling enligt föreskrifterna i 2 kap. TF.

En handling som är påbörjad men som ännu inte har nått sin slutgiltiga form kan innehålla uppgifter som omfattas av sekretess enligt OSL och därför behöver ha ett skydd så att uppgifterna inte röjs för obehöriga. Frågan om en handling är en allmän handling enligt 2 kap. TF är av betydelse då skyddet enligt Försvarsmaktens föreskrifter som rör informationssäkerhet är mindre omfattande för en arbetshandling jämfört med en allmän handling, t.ex. vad gäller exemplarnumrering och kvittering vid mottagande. Kraven på förvaring är dock lika oberoende av vilken status en handling har enligt TF. Det finns därför ett behov att märka arbetshandlingar med en varningssignal om vilket skydd handlingen ska ha.

Det kan understrykas att det inte är möjligt att genom en märkning av handlingen styra om den blir allmän eller inte. Det bestäms av föreskrifterna i TF. Det kan dock vara lämpligt att märka arbetshandlingar med en anteckning, t.ex. UTKAST, så att det under arbetets gång med en handling klart framgår för personer som kommer i kontakt med handlingen att det är en arbetshandling.

9.7.1 Hemliga handlingar

En hemlig handling som inte är allmän skall på första sidan förses med en anteckning om att den är hemlig. Anteckningen får utformas på lämpligt sätt.

2 kap. 1 § tredje stycket Försvarsmaktens föreskrifter om säkerhetsskydd

En hemlig handling skall placeras i en av de informationssäkerhetsklasser som anges i 1 kap. 4 §. Handlingen skall på första sidan förses med en uppgift om i vilken informationssäkerhetsklass den har placerats.

2 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

En arbetshandling som innehåller någon hemlig uppgift ska märkas med informationssäkerhetsklass. Bild 9:15 visar ett exempel på märkning. Märkningen bör vara röd och får göras för hand. Det är tillräckligt att handlingen märks med informationssäkerhetsklass, handlingen får märkas med t.ex. HEMLIG för att särskilt ange att handlingen är hemlig. En sådan anteckning kan vara nödvändig i en verksamhet där främst utrikesklassificerade handlingar hanteras så att handlingarna inte sammanblandas.

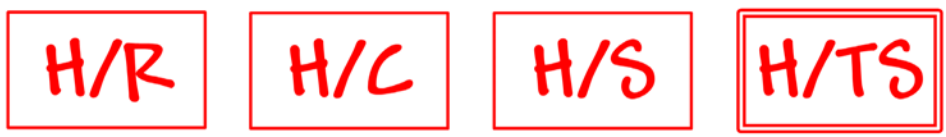


Bild 9:15 - Exempel på märkning med informationssäkerhetsklass på en hemlig handling som är en arbetshandling.

På handlingens första sida eller i anteckningen om att handlingen är hemlig bör datum för handlingens tillkomst anges.

9.7.2 Utrikesklassificerade handlingar

En utrikesklassificerad handling som inte är allmän ska på första sidan förses med en anteckning om att den är utrikesklassificerad. Anteckningen får utformas på lämpligt sätt.

2 kap. 3 § tredje stycket Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

En utrikesklassificerad handling ska i Försvarsmakten märkas med informationssäkerhetsklass.[139]

För att kunna se vilka handlingar som är hemliga respektive utrikesklassificerade ska en utrikesklassificerad handling som är en arbetshandling på första sidan märkas så att det framgår att den är utrikesklassificerad. Ifråga om en elektronisk handling är det lämpligt att beteckningen UTRIKESKLASSIFICERAD används. Ifråga om handlingar som förs för hand är det lämpligt märka handlingen med förkortningen UK. Märkningen bör vara röd och får göras för hand. Bild 9:16 visar ett exempel på sådan märkning.

Bild 9:16 - Exempel på märkning med informationssäkerhetsklass på en utrikesklassificerad handling som är en arbetshandling.

På handlingens första sida eller i anteckningen om att handlingen är utrikesklassificerad bör datum för handlingens tillkomst anges.

9.7.3 Sekretessklassificerade handlingar

En handling som inte är allmän får på första sidan förses med en anteckning om att den är sekretessklassificerad. Anteckningen får utformas på lämpligt sätt.

3 kap. 1 § tredje stycket Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Bild 9:17 - Exempel på märkning på en sekretessklassificerad handling som är en arbetshandling.

Ifråga om en elektronisk handling är det lämpligt att beteckningen SEKRETESSKLASSIFICERAD anges på första sidan för denna anteckning. Ifråga om handlingar som förs för hand är det lämpligt att märka handlingen med förkortningen SK. Märkningen bör vara röd och får göras för hand. Bild 9:17 visar ett exempel på en sådan märkning.

139 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Sekretessklassificerade uppgifter ska inte omfattas av ett säkerhetsskydd och en sekretessklassificerad handling får därför inte placeras i informationssäkerhetsklass.

På handlingens första sida eller i anteckningen om att handlingen är sekretessklassificerad bör datum för handlingens tillkomst anges.

9.8 Registrering

Allmänna handlingar ska registreras så snart de har kommit in till eller upprättats hos en myndighet, om inte annat följer av andra-fjärde styckena.

Om en myndighet hos en annan myndighet har elektronisk tillgång till en upptagning för automatiserad behandling som är en allmän handling ska handlingen registreras endast av den myndighet som gjort upptagningen tillgänglig för den andra myndigheten.

Handlingar som inte omfattas av sekretess behöver inte registreras om de hålls ordnade så att det utan svårighet kan fastställas om de har kommit in eller upprättats.

Om det är uppenbart att en allmän handling är av ringa betydelse för myndighetens verksamhet, behöver den varken registreras eller hållas ordnad.

5 kap. 1 § OSL

I H Säk Sekrbed A beskrivs begreppet allmän handling.

Beträffande handlingar som registreras enligt 1 § ska det av registret framgå

1. datum då handlingen kom in eller upprättades,

2. diarienummer eller annan beteckning handlingen fått vid registreringen,

3. i förekommande fall uppgifter om handlingens avsändare eller mottagare, och

4. i korthet vad handlingen rör.

Uppgifter enligt första stycket 3 eller 4 ska utelämnas eller särskiljas om det behövs för att registret i övriga delar ska kunna hållas tillgängligt för allmänheten.

5 kap. 2 § OSL

Registrering av allmänna handlingar syftar till att garantera allmänhetens rätt att få tillgång till handlingarna. Registreringen är nödvändig för att allmänheten ska kunna få vetskap om vilka handlingar som finns hos en myndighet. Registreringen sker vanligen i ett *diarium*. Diarieföring avser registrering av in- och utgående handlingar i ärenden eller motsvarande. Ett register över allmänna handlingar har normalt också en funktion inom en myndighet så att myndighetens personal ska kunna få vetskap om vilka informationstillgångar som finns inom myndigheten.

Handlingar som innehåller någon uppgift som omfattas av sekretess enligt OSL ska registreras. En allmän handling som inte innehåller någon uppgift som omfattas av sekretess enligt OSL behöver inte registreras om den hålls ordnad så att det utan svårighet kan fastställas om den har kommit in eller upprättats.[140] En myndighet kan dock välja att även registrera sådana handlingar, t.ex. för att underlätta ärendehantering.[141] En myndighet har stor frihet att utforma registreringen av handlingar och ärenden, t.ex. kan flera register användas och innehålla information om handlingar som går utöver minimikraven i 5 kap. 2 § OSL för att garantera allmänhetens insyn i allmänna handlingar.

En allmän handling som har upprättats registreras vid den myndighet som har upprättat handlingen.

Registreringen är inte enbart avsett för pappershandlingar. Även *elektroniska handlingar* som är allmänna handlingar, t.ex. e-post och fotografier, ska registreras.

Ett register över allmänna handlingar kan avse såväl handlingar som inte innehåller uppgifter som omfattas av sekretess som handlingar som omfattas av sekretess. Det finns inget krav på att olika slag av handlingar måste registreras i olika register med avseende på om uppgifterna i handlingarna omfattas av sekretess.

Riksarkivet har beslutat allmänna råd om registrering.[142] Ett register över allmänna handlingar har betydelse för arkivvården[143], bl.a. så att handlingar som har bedömts innehålla någon uppgift som omfattas av sekretess enligt OSL inte lämnas ut från arkiv utan att de först har sekretessgranskats. Även om det i ett register inte framgår att en viss handling har bedömts innehålla någon uppgift som omfattas av sekretess enligt OSL, kan den ändå innehålla sådana uppgifter. Oavsett vad som ur ett sekretessperspektiv är registrerat om en handling, måste handlingen sekretessgranskas innan den lämnas ut.

140 5 kap. 1 § OSL.
141 Sidorna 355-356, Förslag till sekretesslag m.m. prop. 1979/80:2 Del A.
142 Riksarkivets allmänna råd om registrering.
143 5 § arkivlagen.

Diarium vid myndigheter under försvarsdepartementet ska bevaras, de får inte gallras.[144]

9.8.1 Undantag från registrering

Vissa slag av allmänna handlingar som förekommer hos en myndighet i stor omfattning kan av regeringen undantas från registreringsskyldigheten.[145] Ett skäl till denna möjlighet är att det kan komma att bli utomordentligt betungande för myndigheten att registrera handlingarna. T.ex. har regeringen undantagit patientjournaler i Försvarsmakten, som rör totalförsvarspliktiga och anställd personal, från kravet att de ska registreras.[146]

9.8.2 Utelämna eller särskilja uppgifter i register p.g.a. sekretesskäl

Vanligen innehåller ett register över allmänna handlingar inte några uppgifter som omfattas av sekretess enligt OSL. I vissa fall kan en uppgift i ett diarium träffas av sekretessbestämmelser i OSL. I sådana fall ska uppgiften om handlingens avsändare och mottagare eller beskrivning av handlingens innehåll (ärendemening) inte föras in i registret. Alternativt kan uppgifterna särskiljas. Registret ska i övrigt kunna vara tillgängligt för allmänheten.[147] Om uppgifterna om handlingens avsändare och mottagare eller ärendemening ska särskiljas registreras uppgifterna i ett separat register. Normalt behöver det då finnas en hänvisning i det för allmänheten tillgängliga registret som pekar på var uppgifterna finns.

Om en handlings avsändare och mottagare eller ärendemening innehåller en uppgift som omfattas av sekretess enligt OSL ska fortfarande datum då handlingen kom in eller upprättades samt diarienummer, eller annan beteckning som handlingen fått vid registreringen, föras in i det register som är tillgängligt för allmänheten. Existensen av en allmän handling får inte undanhållas allmänheten, även om uppgifterna om handlingen i registret som allmänheten har insyn i kan vara begränsade.

Ett register som innehåller uppgifter som omfattas av sekretess enligt OSL ska ges det skydd som motsvarar uppgifternas skyddsvärde. T.ex. ska ett sådant register ges ett säkerhetsskydd om det innehåller hemliga uppgifter.

144 2 § Riksarkivets föreskrifter om gallring av handlingar rörande hanteringen av hemliga och kvalificerat hemliga handlingar hos myndigheter under Försvarsdepartementet.

145 5 kap. 3 § OSL.

146 2 § OSF.

147 5 kap. 2 § andra stycket OSL.

9.8.3 Register som är undantagna allmänhetens insyn

Inom vissa områden eller för vissa slag av handlingar skulle ett register över allmänna handlingar p.g.a. sekretess enligt OSL endast komma att innehålla datum då handlingarna kom in eller upprättades samt diarienummer. Regeringen får för ett visst register föreskriva att uppgifter om handlingarnas avsändare och mottagare eller beskrivning av handlingens innehåll (ärendemening) *inte* får utelämnas eller särskiljas.[148] Uppgifterna om en handlings avsändare och mottagare eller ärendemening ska då registreras i registret även om de omfattas av sekretess enligt OSL. Då registret kommer att innehålla uppgifter som omfattas av sekretess enligt OSL kan registret inte hållas tillgängligt för allmänheten. Existensen av ett sådant register är inte en uppgift som omfattas av sekretess enligt OSL då sådana register är angivna i 3 § OSF. Allmänheten kan begära att få ta del av registret och då måste en sekretessprövning göras på samma sätt som för en allmän handling som begärs utlämnad. En positiv effekt ur säkerhetssynpunkt med separata register som allmänheten p.g.a. sekretesskäl inte har insyn i är att tillgången till ett sådant register även ska begränsas inom myndigheten till de personer som behöver tillgång till registret. Det kan även vara nödvändigt att styra behörigheten till uppgifterna i ett sådant register med hänsyn till vilka uppgifter personerna är behöriga till.

Om regeringen har föreskrivit att ett visst register alltid ska innehålla handlingarnas avsändare och mottagare eller ärendemening får registret endast användas för registrering av handlingar som uppfyller de villkor som regeringen föreskrivit. Andra slag av allmänna handlingar ska registreras i ett annat register, normalt ett register som är tillgängligt för allmänheten.

Ett exempel på register över allmänna handlingar som regeringen har undantagit från allmänhetens insyn är diarier vid Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets forskningsinstitut över underrättelser inom försvarets underrättelse- och säkerhetstjänst.[149] Registret är även avsett för inriktningar enligt lagen om försvarsunderrättelseverksamhet. Registret får således endast användas för registrering av allmänna handlingar som är sådana underrättelser eller inriktningar. Alla andra slag av allmänna handlingar i underrättelse- och säkerhetstjänst ska registreras i ett register som allmänheten har insyn i. Detta undantag från allmänhetens insyn i sådana register är i Försvarsmakten inte begränsat till MUST, utan ska i Försvarsmakten även tillämpas av organisationsenheter.

9.8.4 Registrering som en skyddsåtgärd

Registrering är av stor betydelse för informationssäkerheten då den gör det möjligt att upprätthålla kontrollen över en handling eller ett lagringsmedium under deras livscykel,

148 5 kap. 4 § OSL.
149 3 § OSF.

från att dessa har kommit in eller upprättats till dess att de har förstörts. Genom registrering skapas underlag för inventering av handlingar och lagringsmedier för att kontrollera om handlingarna och lagringsmedierna fortfarande är i behåll eller om de har förlorats. Registret ger även underlag för vilka handlingar och lagringsmedier som ska förstöras efter att de har återlämnats. Ett register över handlingar som innehåller hemliga uppgifter behövs även för att i efterhand kunna avgöra vilka handlingar som en person har haft tillgång till, t.ex. som underlag i en utredning om spioneri.

I det register där en allmän handling som är hemlig och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre är diarieförd skall anges vem som förvarar handlingen eller om handlingen har förkommit eller gallrats.

2 kap. 19 § Försvarsmaktens föreskrifter om säkerhetsskydd

Uppgifterna ska anges i det register där handlingen är diarieförd, uppgifterna får alltså inte anges i något annat register.

Det finns ur säkerhetssynpunkt inget krav på att det i ett register ska anges vem som förvarar en hemlig handling som är en allmän handling och som är placerad i informationssäkerhetsklass HEMLIG/RESTRICTED. På samma sätt finns inget krav på att det i ett register ska anges om en sådan handling har förkommit eller gallrats.[150] Det kan dock finnas andra skäl för att i ett register ändå ange vem som förvarar en sådan handling. I det fall det inte finns något arkivexemplar kan en myndighet välja att ange vem som förvarar en sådan handling för att myndigheten ska kunna lokalisera handlingar, t.ex. för att skyndsamt kunna hantera ärenden om utlämnande av allmän handling.

Avsnitt 9.8.5 beskriver sekretess för sammanställningar över vem som förvarar hemliga handlingar och lagringsmedier.

Är en allmän handling som är hemlig placerad i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre skall det på sändlistan till handlingen eller i det register där handlingen är diarieförd anges hur många exemplar av handlingen som har framställts och vilka som är mottagare av respektive exemplar.

2 kap. 7 § Försvarsmaktens föreskrifter om säkerhetsskydd

150 2 kap. 19 § Försvarsmaktens föreskrifter om säkerhetsskydd.

En handling kan finnas i flera exemplar. Ur säkerhetssynpunkt är det nödvändigt att upprätthålla kontrollen över *varje exemplar* för allmänna handlingar som är hemliga handlingar och som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre. För en handling som är placerad i informationssäkerhetsklass HEMLIG/RESTRICTED finns inget krav på exemplarnumrering och kvittering varför registret inte ska innehålla uppgifter om hur många exemplar som har framställts av handlingen och vilka som är mottagare av respektive exemplar.

> *Har en kopia av eller ett utdrag ur en allmän handling som är hemlig och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre gjorts, skall uppgift om detta liksom uppgift om till vem kopian eller utdraget har lämnats antecknas i register eller liggare.*
>
> 2 kap. 10 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

För att säkerställa spårbarheten behöver även kopior av eller utdrag ur en allmän handling som är en hemlig handling och som är placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre antecknas i registret. Det är lämpligt att det register där handlingen är diarieförd även innehåller uppgifter om kopior och utdrag. En kopia av en handling utgör ett nytt exemplar av handlingen. Ett utdrag ur handlingen utgör en ny handling som ska registreras.

9.8.5 Sekretess för sammanställningar över vem som förvarar hemliga handlingar och lagringsmedier

Sammanställningar av uppgifter i ett register om *vem* som innehar hemliga handlingar och lagringsmedier kan ge underrättelseaktörer vägledning om vilka personer vid en svensk myndighet som utgör informationsbärare. Sådana sammanställningar visar också vilka personer som har åtkomst till uppgifter som svarar mot underrättelseaktörernas inhämtningsbehov.

Hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET kan förutsättas vara av störst intresse för en underrättelseaktör. Då behörigheten att ta del av hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET normalt är begränsad inom en myndighet (avsnitt 7.3) bör sådana sammanställningar omfattas av sekretess enligt 15 kap. 2 § OSL. Ett röjande av en sådan sammanställning leder i sig inte till ett omedelbart röjande av uppgifterna i de registrerade handlingarna och lagringsmedierna. Däremot underlättas underrättelseaktörernas målsökning av personal. Ett röjande av en sådan sammanställning bedöms därför endast ge ett ringa men varför den placeras i informationssäkerhetsklass HEMLIG/RESTRICTED.

En sammanställning över vem som innehar hemliga handlingar och lagringsmedier som är placerade i informationssäkerhetsklasserna HEMLIG/CONFIDENTIAL och HEMLIG/SECRET bör omfattas av sekretess enligt 18 kap. 8 § fjärde punkten OSL. I Försvarsmakten informationsklassificeras en sådan sammanställning som en sekretessklassificerad handling.

Ett register över allmänna handlingar där hemliga handlingar diarieförs ska innehålla uppgift om vem som förvarar en sådan handling som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre (avsnitt 9.8.4).[151] Ett sådant register är ett exempel på en sammanställning som beskrivits ovan. Sekretess för sammanställda uppgifter om vem som förvarar hemliga handlingar och lagringsmedier hindrar inte att övriga uppgifter i ett sådant register är tillgängligt för allmänheten (se även avsnitten 9.8-9.8.3).

En inventering av hemliga handlingar och lagringsmedier utgår vanligtvis från en förteckning per person med en sammanställning av de handlingar och lagringsmedier som har registrerats på den personen (s.k. inventeringslista). En inventeringslista är ytterligare ett exempel på en sammanställning som beskrivits ovan.

En åtgärd för att förhindra röjande av sammanställningarna är att använda *handläggarkoder*, som då ersätter identifieringsuppgift (namn och personnummer) i ett register. Om handläggarkoder används är det lämpligt att samtliga koder ändras vart tredje år. En annan åtgärd då ett register förs i ett IT-system är att använda säkerhetsfunktionen för *behörighetskontroll* för att styra vilka uppgifter i ett register som kan läsas av användarna.

151 2 kap. 19 § Försvarsmaktens föreskrifter om säkerhetsskydd.

9.9 Kvittering vid mottagande

Kvittering vid mottagande av hemliga handlingar är en skyddsåtgärd dels för att skydda den anställde, dels som ett skydd för myndighetens handlingar. Vilka regler som gäller vid kvittering är knutna till vilken informationssäkerhetsklass det rör och i vissa fall om en handling är att anses som allmän eller inte. Kvittering möjliggör spårbarhet av vilka personer som tagit del av hemliga uppgifter i skrift eller bild. Kvittering och den registrering som sker av hemliga handlingar är väsentligt för att veta vem som innehar en viss hemlig handling.

Tabellen visar vilka krav som finns i fråga om kvittering vid mottagande av en hemlig handling.

<table>
<tr><th>Informationssäkerhetsklass</th><th>Allmän handling</th><th>Arbets-handling</th><th>Krav på kvittering</th></tr>
<tr><td>HEMLIG/TOP SECRET</td><td>X</td><td>X</td><td>Mottagandet kvitteras med namnteckning och namnförtydligande på ett särskilt kvitto med kopia. När en sådan handling återlämnas ska detta antecknas på kvittokopian, som ska bevaras hos myndigheten i minst 25 år.[152]</td></tr>
<tr><td>HEMLIG/SECRET</td><td rowspan="2">X</td><td rowspan="2"></td><td rowspan="2">Mottagandet kvitteras med namnteckning och namnförtydligande. Kvittensen ska bevaras hos myndigheten i minst 10 år.[152]</td></tr>
<tr><td>HEMLIG/CONFIDENTIAL</td></tr>
<tr><td>HEMLIG/SECRET</td><td rowspan="2"></td><td rowspan="2">X</td><td rowspan="3">Ska inte kvitteras.[152]</td></tr>
<tr><td>HEMLIG/CONFIDENTIAL</td></tr>
<tr><td>HEMLIG/RESTRICTED</td><td>X</td><td>X</td></tr>
</table>

Kvittering ska ske genom att mottagaren skriver sin *fullständiga namnteckning med namnförtydligande* på kvittot. Vidare är det självklart att *datum* för kvittering anges på kvittot.

Det är lämpligt att det vid expedition eller motsvarande finns en förteckning med namnteckningar på den personal som är behöriga att ta del av hemliga handlingar. Förteckningen bör uppdateras en gång per år (se även avsnitt 7.5 om behörighetsförteckning).

Att kvitto ska bevaras hos myndigheten 10 respektive 25 år är kopplat till preskriptionstiden för brott.[153] T.ex. är preskriptionstiden 10 år för grov obehörig befattning med hemlig handling.[154]

152 2 kap. 11 § Försvarsmaktens föreskrifter om säkerhetsskydd.
153 35 kap. 1 § brottsbalken.
154 19 kap. 8 § brottsbalken.

Om en person vägrar att kvittera ett mottagande av en hemlig handling som är placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre får handlingen inte lämnas till personen. Personal vid myndigheter som inte har ett så väl utvecklat säkerhetsskydd kan uttrycka förvåning och starka protester då de i Försvarsmakten ska kvittera ett mottagande av en hemlig handling. Ofta finns det en missuppfattning att kvitteringen sker p.g.a. missförtroende för personen eller den andra myndigheten. Det är av stor vikt att sådan personal ges kompletterande utbildning, t.ex. av en säkerhetschef, så att några missförstånd i frågan inte förekommer.

9.9.1 Underkvittering

Då en hemlig eller utrikesklassificerad handling som är placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre behöver lånas av en annan anställd kan handlingen tillfälligt lämnas över till personen som vid mottagandet kvitterar handlingen. Denna *underkvittering* kan ske på det befintliga kvittot eller så upprättar personerna på enklaste sätt ett nytt kvitto. Kvittot behåller den ursprungliga innehavaren av handlingen, som måste kunna visa upp det istället för den utlånade handlingen. När handlingen lämnas tillbaka byts kvittot mot handlingen. Personen som lånade handlingen ska på ett delgivningskvitto eller lista kvittera att han eller hon har tagit del av uppgifter i handlingen (avsnitt 9.10).

Ett lån av en handling som är placerad i informationssäkerhetsklass HEMLIG/RESTRICTED ska inte kvitteras.

En person som lånar en hemlig eller utrikesklassificerad handling ska vara behörig att ta del av uppgifterna i handlingen (kapitel 7). Självklart gäller att handlingen ska förvaras enligt vad som gäller för den informationssäkerhetsklass som handlingen är placerad i (avsnitt 9.11).

Underkvittering av handlingar som är placerad i informationssäkerhetsklass HEMLIG/TOP SECRET bör undvikas, det är ur säkerhetssynpunkt bättre att alla sådana handlingar hanteras via en expedition.

9.9.2 Mellankvittering

Med *mellankvittering* avses den kvittering som en eller flera personer gör för att hantera en hemlig eller utrikesklassificerad handling, som är placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre, innan handlingen når den person som ska läsa den. Ett exempel på när mellankvittering används är i de fall det inte är möjligt för en person att själv hämta en hemlig eller utrikesklassificerad handling vid en expedition. I dessa fall kan en annan anställd, t.ex. en sekreterare, ha till arbetsuppgift att hämta personens handlingar vid en expedition. Den person som hämtar handlingen kvitterar mottagandet vid expeditionen men denna kvittering sägs vara

en mellankvittering då den kvitterande personen inte är den som ska läsa handlingen. Mellankvittering används t.ex. för vissa ledamöter i Försvarsmaktens ledningsgrupp.[155]

En handling som är placerad i informationssäkerhetsklass HEMLIG/RESTRICTED ska inte mellankvitteras.

Mellankvittering av handlingar som är placerad i informationssäkerhetsklass HEMLIG/TOP SECRET bör undvikas, det är ur säkerhetssynpunkt bättre att en person som ska ta emot en sådan handling personligen kvitterar handlingen vid en expedition.

9.9.3 Arkiv- och expeditionspersonal

Arkiv- och expeditionspersonal behöver inte kvittera när de tar emot en hemlig handling för *registrering*, *kopiering*, *arkivering* eller *förstöring*, om inte den som lämnar över handlingen begär det.[156] Orsaken till detta undantag är bl.a. att arkiv- och expeditionspersonal dagligen tar emot en stor del hemliga handlingar t.ex. för registrering. Arkiv- och expeditionspersonalen får därmed anses ha haft möjlighet att ta del av de hemliga uppgifterna och därmed är det inte heller rationellt att upprätthålla kvitteringskravet för denna personalkategori.

När personal som har till uppgift att kopiera en hemlig handling tar emot en hemlig handling från expeditionspersonal för att mångfaldiga den får de anses utföra en arbetsuppgift som ankommer på expeditionspersonalen. Tryckeripersonal behöver i en sådan situation därför inte kvittera handlingen.

När hemliga handlingar överlämnas till ett arkiv, inom Försvarsmakten eller till Krigsarkivet, behöver således inte handlingarna kvitteras av arkivpersonalen. Även om en hemlig handling senare skulle saknas finns det inte någon praktisk möjlighet att genom ett kvittensförfarande kräva ansvar för den förlorade handlingen. Om en hemlig handling saknas vid en expedition eller ett arkiv ska förhållandet säkerhetsrapporteras.[157]

9.9.4 Utrikesklassificerade handlingar

Kraven på kvittering vid mottagande av hemliga handlingar gäller i Försvarsmakten även för utrikesklassificerade handlingar.[158]

155 4 kap. 9 § Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).
156 2 kap. 11 § tredje stycket Försvarsmaktens föreskrifter om säkerhetsskydd.
157 4 kap. 2 § Försvarsmaktens föreskrifter för Försvarsmaktens personal.
158 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

9.9.5 Sekretessklassificerade handlingar

Mottagande av en sekretessklassificerad handling ska inte kvitteras i Försvarsmakten.[159]

9.10 Muntlig delgivning eller visning

9.10.1 Hemliga handlingar

> *Varje myndighet skall besluta hur kvittering skall göras om uppgifter i en hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET lämnas muntligt eller genom visning.*
>
> 2 kap. 12 § Försvarsmaktens föreskrifter om säkerhetsskydd

Hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET hör till de mest skyddsvärda informationstillgångarna vid en myndighet. Det är därför lämpligt att kvittering ska ske när uppgifter ur en hemlig handling som är placerad i informationssäkerhetsklass HEMLIG/TOP SECRET delges muntligt eller genom visning. Kvittering bör göras genom namnteckning och namnförtydligande på ett delgivningskvitto eller en lista. Det är även lämpligt att ange datum för kvittering på delgivningskvittot eller listan.

Föreskriften gäller såväl för allmänna handlingar som handlingar som inte är allmänna (s.k. arbetshandlingar). Ett beslut enligt föreskriften kan framgå i en myndighets interna föreskrifter om säkerhetsskydd.[160]

> *Om uppgifter i en allmän hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre lämnas muntligt eller genom visning ska kvittering genom namnteckning och namnförtydligande ske på delgivningskvitto eller lista. Detsamma ska gälla även i fråga om uppgifter i en hemlig handling som inte är allmän och som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET.*
>
> *På delgivningskvittot eller listan ska anges det datum informationen lämnades. Kvittot eller listan ska om möjligt förvaras tillsammans med handlingen.*
>
> 2 kap. 4 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

159 Föreskrift om kvittering saknas i 3 kap. Försvarsmaktens föreskrifter om skydd för utrikes- och sekretess klassificerade uppgifter och handlingar.

160 45 § säkerhetsskyddsförordningen.

Spårbarhet för vem som har tagit del av hemliga uppgifter gäller i Försvarsmakten inte enbart vem som har tagit emot en hemlig handling i pappersform. Uppgifter ur hemliga handlingar delges även muntligt eller genom visning och motsvarande spårbarhet ska då säkerställas genom kvittering. Det ska vara naturligt att be en person kvittera då uppgifter ur en handling delges muntligt eller genom visning. Lika naturligt ska det vara för en person, t.ex. en chef, som delges uppgifter ur en handling att fråga efter delgivningslistan.

Kravet på en sådan kvittering gäller inte för uppgifter ur en hemlig handling som är placerad i informationssäkerhetsklass HEMLIG/RESTRICTED. Kravet gäller heller inte för uppgifter ur en hemlig handling som inte är en allmän handling, förutom i fråga om HEMLIG/TOP SECRET. Delgivning av uppgifter ur en handling som är placerad i informationssäkerhetsklass HEMLIG/TOP SECRET ska, som framgår av föreskriften, alltid kvitteras.

Det är lämpligt att en expedition alltid fäster en delgivningslista på hemliga handlingar som är allmänna handlingar och som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre. På så sätt behöver inte innehavaren av en sådan handling tänka på att finna en sådan blankett i samband med att delgivning av uppgifter ur handlingen ska ske. På motsvarande sätt är det lämpligt att en expedition även fäster en delgivningslista på hemliga handlingar som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET och som inte är en allmän handling.

Kravet på kvittering gäller även i mötessammanhang där uppgifter ska presenteras muntligt eller genom visning. Kravet på kvittering gäller för hemliga handlingar i informationssäkerhetsklass HEMLIG/CONFIDENTIAL och HEMLIG/SECRET endast i det fall presentationen uppfyller villkoren i TF för att vara en allmän handling, t.ex. om en presentation har färdigställts, och därmed upprättats, för mötet.

I fråga om muntlig delgivning eller genom visning av uppgifter ur en hemlig handling gäller i Försvarsmakten krav enligt tabellen nedan.

<table>
<tr><th>Informationssäkerhetsklass</th><th>Allmän handling</th><th>Arbets-handling</th><th>Krav på kvittering vid delgivning</th></tr>
<tr><td>HEMLIG/TOP SECRET</td><td>X</td><td>X</td><td rowspan="3">Delgivning kvitteras genom namnteckning och namnförtydligande på delgivningskvitto eller lista. Datum då informationen lämnandes ska anges på delgivningskvittot eller listan. Kvittot eller listan ska om möjligt förvaras tillsammans med handlingen.[161]</td></tr>
<tr><td>HEMLIG/SECRET</td><td rowspan="2">X</td><td rowspan="2"></td></tr>
<tr><td>HEMLIG/CONFIDENTIAL</td></tr>
<tr><td>HEMLIG/SECRET</td><td rowspan="2"></td><td rowspan="2">X</td><td rowspan="3">Delgivning ska inte kvitteras.[161]</td></tr>
<tr><td>HEMLIG/CONFIDENTIAL</td></tr>
<tr><td>HEMLIG/RESTRICTED</td><td>X</td><td>X</td></tr>
</table>

Det är lämpligt att delgivningslistan för ett möte är en del av mötets närvarolista. En sådan lista måste då tas om hand efter mötet då listan blir en allmän handling. Av listan måste det även framgå vilket möte och vilka hemliga handlingar som listan avser.

9.10.2 Utrikesklassificerade handlingar

Kvittering vid muntlig delgivning eller genom visning av uppgifter ur en utrikesklassificerad handling ska i Försvarsmakten ske på samma sätt som för en hemlig handling.[162]

9.10.3 Sekretessklassificerade handlingar

Muntlig delgivning eller visning av uppgifter ur en sekretessklassificerade handlingar ska inte kvitteras i Försvarsmakten.[163]

9.11 Förvaring

Av informationssäkerhetens betydelse för säkerhetsskyddet följer att hemliga handlingar måste förvaras så att obehöriga inte kan ta del av deras innehåll och så att de inte ska kunna tillgripas.

161 2 kap. 4 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd viss materiel.
162 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.
163 Föreskrift om kvittering saknas i 3 kap. Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

9.11.1 Skyddsnivåer för förvaringsutrymmen

Beroende på vilket men uppgifterna i de hemliga handlingarna kan orsaka om de röjs till obehörig, vilket framgår av den informationssäkerhetsklass som de har placerats i, ska handlingarna förvaras i förvaringsutrymmen som under viss tid motstår försök till intrång. Förvaringsutrymmena indelas i fyra skyddsnivåer. Ju kraftigare konstruerade utrymmena är och därmed sammanhängande förmåga att motstå angrepp desto högre skyddsnivå har de. Ju högre informationssäkerhetsklass en hemlig handling är placerad i, desto kraftigare konstruerat ska förvaringsutrymmet vara, d.v.s. ha en viss skyddsnivå.

Ett förvaringsutrymme för hemliga handlingar ska uppfylla de krav som gäller för respektive skyddsnivå. Krav på förvaringsutrymme för respektive skyddsnivå framgår av bilaga till Försvarsmaktens föreskrifter om säkerhetsskydd.[164] Tabellen visar vilken skyddsnivå som ett förvaringsutrymme ska ha för förvaring av hemliga handlingar samt kommentar till krav på förvaringen.

Informationssäkerhetsklass	Skyddsnivå	Kommentar
HEMLIG/TOP SECRET	4[165]	Förvaringsutrymme kan utgöras av värdeskåp, valv etc.
HEMLIG/SECRET	3[166]	Förvaringsutrymme kan t.ex. utgöras av säkerhetsskåp (enligt SS 3492), värdeskåp (enligt SS-EN 1143-1), säkerhetsarkiv etc.
HEMLIG/CONFIDENTIAL		
HEMLIG/RESTRICTED	1[167]	Förvaringsutrymme kan utgöras av sektionerade lokaler inom en stab eller av ett låst tjänsterum etc. Utrymmet ska då hållas låst och endast den personal som är behörig att ta del av handlingen får ha tillträde till utrymmet (berör tillfälliga besökare, lokalvårdare etc. som inte är behöriga).[167]

Skyddsnivå 2 har inte använts för kravställning av förvaringsutrymmen för hemliga handlingar. Skyddsnivå 2 används dock för krav på andra utrymmen, t.ex. för IT- och telekommunikation.[168]

164 2 kap. 13 § Försvarsmaktens föreskrifter om säkerhetsskydd.
165 2 kap. 16 § Försvarsmaktens föreskrifter om säkerhetsskydd.
166 2 kap. 15 § Försvarsmaktens föreskrifter om säkerhetsskydd.
167 2 kap. 14 § Försvarsmaktens föreskrifter om säkerhetsskydd.
168 3 kap. 9 och 10 §§ Försvarsmaktens föreskrifter om säkerhetsskydd.

9.11.2 Beslut om avvikelse från krav på förvaring

Varje myndighet får fatta beslut som avviker från föreskrifterna i 14-16 §§ i detta kapitel under förutsättning att motsvarande skyddsnivå kan upprätthållas. Ett sådant beslut skall dokumenteras.

2 kap. 17 § Försvarsmaktens föreskrifter om säkerhetsskydd

Varje myndighet får, med hänsyn till

- de lokala förutsättningarna,
- de aktuella utrymmenas eller lokalernas geografiska placering,
- de aktuella utrymmenas eller lokalernas utförande,
- möjligheter att larma eller på annat sätt övervaka utrymmenas eller lokalernas skalskydd,
- möjligheter att med insatsstyrka kunna ingripa innan intrång skett i utrymmena eller lokalerna m.m.,

fatta beslut som avviker från föreskrifterna i 2 kap. 14-16 §§ Försvarsmaktens föreskrifter om säkerhetsskydd. Det bör poängteras att beslut om avvikelse från föreskrifterna bara får fattas om det innebär att *motsvarande skyddsniv*å kan upprätthållas. Inför ett beslut om avvikelse bör en säkerhetsanalys ha genomförts. Ett sådant beslut ska dokumenteras.

Beslut som en chef för en organisationsenhet fattar om var och hur hemliga handlingar ska förvaras ska grundas på en bedömning av tillträdesbegränsningens utformning, förvaringsplatsens belägenhet, sannolikheten för upptäckt av ett tillgrepp och insatstid för att förhindra ett tillgrepp.

2 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

I Försvarsmakten är det chefen för en organisationsenhet som får fatta beslut som avses i 2 kap. 17 § Försvarsmaktens föreskrifter om säkerhetsskydd. Ett exempel på sådant beslut kan vara att i förvaringsutrymmen eller lokaler som bara uppfyller skyddsnivå 3 förvara hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET, trots att krav på skyddsnivå 4 föreligger. Ett sådant beslut kan fattas om utrymmets skalskydd (golv, väggar, tak, dörr) förses med seismiska detektorer och en insatsstyrka kan ingripa, på plats, innan intrång i utrymmet eller lokalen skett, d.v.s. i regel inom tio minuter.

Ett annat exempel på ett sådant beslut kan vara ett föremål som genom sitt omfång inte kan förvaras i rekommenderat förvaringsutrymme. Detta kan exempelvis gälla för en översiktskarta i en stabslokal. Stabslokalens utformning, tillträdesbegränsning och bemanning är faktorer i bedömningen om förvaringen kan uppnå motsvarande skyddsnivå som det rekommenderade förvaringsutrymmet. Förvaringen av översiktskartan i stabslokalen måste uppnå motsvarande säkerhetsskydd som ett förvaringsutrymme som uppfyller kraven för den skyddsnivå som den informationssäkerhetsklass som översiktskartan är placerad i.

Det är däremot normalt inte möjligt att fatta beslut om att förvaring som kräver utrymme eller lokal i skyddsnivå 3, får ske i ett skalskyddslarmat utrymme eller lokal i skyddsnivå 2 och att insats ska kunna ske innan intrång i utrymmet eller lokalen skett. Detta beroende på att en insatsstyrka som regel inte hinner ingripa inom sådan tid och att intrång i utrymmet eller lokalen skett, d.v.s. vanligtvis inom fem minuter.

9.11.3 Åtskild förvaring

Handlingar som inte innehåller hemliga uppgifter ska om möjligt förvaras åtskilda från hemliga handlingar. Hemliga handlingar som är placerade i informationssäkerhetsklassen HEMLIG/SECRET eller lägre ska om möjligt förvaras åtskilda från hemliga handlingar som är placerade i informationssäkerhetsklassen HEMLIG/TOP SECRET.

2 kap. 6 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Syftet med åtskild förvaring är att handlingarna inte ska sammanblandas så att de förloras i den vidare hanteringen. En sammanblandning kan leda till att uppgifterna i de hemliga handlingarna röjs, t.ex. genom rensning av arbetshandlingar. Ytterligare ett syfte är att underlätta inventering av de hemliga handlingarna.

Med om möjligt avses att handlingarna får förvaras tillsammans om de t.ex. hör till ett och samma ärende. Det är lämpligt att i sådana fall använda pärmar där förekomsten av hemliga handlingar antecknas på en innehållsförteckning i pärmen. Ett annat sätt är att alltid använda en röd plastmapp för varje hemlig handling. Bild 9:18 illustrerar innebörden av föreskriften.

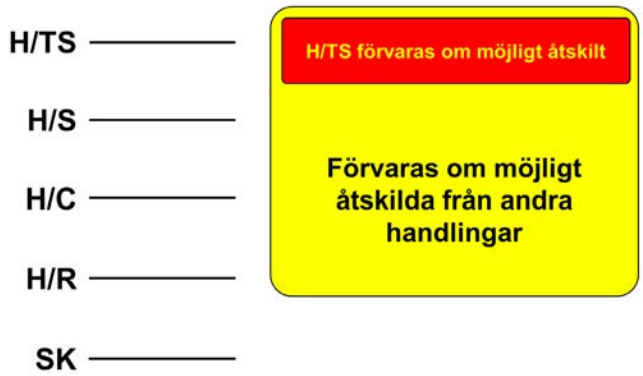


Bild 9:18 - Schematisk beskrivning av åtskild förvaring.

9.11.4 Att lämna handlingar framme

> *Om en myndighet har beslutat att anställda under kortare tid får lämna hemliga handlingar framme i ett låst arbetsrum, skall huvudnycklar och reservnycklar förvaras så att inte någon obehörig kan komma åt dem.*
>
> 2 kap. 18 § Försvarsmaktens föreskrifter om säkerhetsskydd

Om personal ska få medges att under kortare tid, t.ex. under lunch, få lämna hemliga handlingar framme i arbetsrummet och inte behöva låsa in dem i ett förvaringsutrymme måste man säkerställa att inga obehöriga har tillgång till nycklar till det låsta arbetsrummet. Detta innebär att nycklar, inklusive huvudnycklar, måste förvaras på ett säkert sätt. Nycklar ska stå under uppsikt eller vara inlåsta i ett utrymme med samma skyddsnivå som det arbetsrum för vilka de är avsedda.

Skyddsåtgärden gäller även i fråga om lagringsmedier, t.ex. en klienthårddisk för ett IT-system som är avsett för behandling av hemliga uppgifter.[169]

I Försvarsmakten ska nycklar som inte används förvaras i förseglat emballage.[170] Under den tid hemliga handlingar lämnas framme i arbetsrummet ska arbetsrummet hållas låst. Det bör av arbetsordning eller motsvarande framgå om personalen får lämna hemliga handlingar framme i låst arbetsrum samt vad som avses med kortare tid.

169 7 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd.
170 3 kap. 7 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

9.11.5 Förvaringsutrymme i fordon

När en enskild befattningshavare regelbundet medför hemliga handlingar till hemliga anläggningar ska, om fordon används, detta vara utrustat med ett fast monterat förvaringsutrymme med en skyddsnivå motsvarande ett säkerhetsskåp enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 3492.

2 kap. 29 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Med hemliga anläggningar avses anläggningar där anläggningens geografiska position omfattas av sekretess enligt 15 kap. 2 § OSL. Behov i andra fall av förvaringsutrymme för hemliga handlingar i fordon bör uppmärksammas i säkerhetsplanering för en verksamhet.

För transport av hemliga handlingar finns ytterligare föreskrifter i 2 kap. 21-22, 24-29 och 30-35 §§ Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

9.11.6 Utrikesklassificerade handlingar

Förvaring av utrikesklassificerade handlingar och materiel som innehåller utrikesklassificerade uppgifter ska i Försvarsmakten ske på samma sätt som för hemliga handlingar.[171]

9.11.7 Nato-handlingar

Nato brukar vid inspektioner i Sverige ge uttryck för uppfattningen att Nato-handlingar ska förvaras avskilt. Det är därför lämpligt att Nato-handlingar där det är möjligt förvaras åtskilt från andra handlingar. I arkiv kan den avskilda förvaringen ske i ett säkerhetsskåp som placeras i arkivlokalen.

För Nato-handlingar som förvaras av en anställd bör handlingarna förvaras åtskilda från andra handlingar, d.v.s. som vid åtskild förvaring av hemliga handlingar (avsnitt 9.11.3).

171 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

9.11.8 Sekretessklassificerade handlingar

En sekretessklassificerad handling som inte står under uppsikt ska förvaras inlåst.

Ett förvaringsutrymme för sådana handlingar ska uppfylla de krav som gäller för lägst skyddsnivå 1 enligt bilaga 1 till Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd.

3 kap. 4 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

En sekretessklassificerad handling ska förvaras inlåst. Det är alltså tillräckligt att en sådan handling förvaras t.ex. i en låst skrivbordshurts eller i en pärm i ett låst jalusiskåp på arbetsplatsen. Även ett låst arbetsrum är tillräckligt skydd, under förutsättning att endast personer som är behöriga att ta del av handlingarna har nyckel eller på annat sätt tillgång till rummet. Detta utesluter inte att handlingen får förvaras i ett förvaringsutrymme som uppfyller krav på skyddsnivå 2 eller högre. Om en sekretessklassificerad handling förvaras i ett sådant utrymme ska handlingen om möjligt förvaras åtskild från hemliga och utrikesklassificerade handlingar (se avsnitt 9.11.3).

Krav på att ett förvaringsutrymme ska uppfylla de krav som gäller för lägst skyddsnivå 1 motsvarar det krav som gäller för förvaring av en hemlig handling som har placerats i informationssäkerhetsklass HEMLIG/RESTRICTED. Vid utformning av skyddet för sekretessklassificerade handlingar (även lagringsmedier) ska normalt inte förvaringsutrymmen som anskaffas och som endast är tänkt att användas för förvaring av sekretessklassificerade handlingar uppfylla krav på skyddsnivå 2 eller högre.

Varje organisationsenhet får fatta beslut som avviker från föreskriften i 4 § i detta kapitel under förutsättning att motsvarande skyddsnivå kan upprätthållas. Ett sådant beslut ska dokumenteras.

3 kap. 5 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Varje organisationsenhet får med hänsyn till:

- de lokala förutsättningarna,
- de aktuella utrymmenas eller lokalernas geografiska position, och
- de aktuella utrymmenas eller lokalernas utförande

fatta beslut som avviker från föreskriften med krav på skyddsnivå 1. Avvikelse får dock bara fattas om beslutet innebär att *motsvarande skyddsniv*å kan vidmakthållas.

9.12 Samförvaring

9.12.1 Hemliga handlingar

> *Chef för organisationsenhet, eller den han eller hon bestämmer, får besluta att ett förvaringsutrymme får användas gemensamt av flera personer. Ett sådant samförvaringsbeslut ska dokumenteras.*
>
> 2 kap. 7 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Samförvaring avser enbart förvaringen av hemliga handlingar. Samförvaringen innebär inte att personerna, som gemensamt får använda ett förvaringsutrymme, är behöriga att ta del av varandras handlingar. Samförvaring är inte lämpligt då flera personer från skilda verksamheter gemensamt ska förvara hemliga handlingar som de sinsemellan inte är behöriga till. Samförvaring är inte lämpligt för handlingar som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET.

Grunden för förvaring av hemliga handlingar är att varje person förvarar de hemliga handlingarna i ett förvaringsutrymme som endast den person som kvitterat de hemliga handlingarna kan komma åt. Kostnader för förvaringsutrymmen är små i förhållande till de skyddsvärden uppgifterna i de hemliga handlingarna representerar och som oftast inte kan mätas i ekonomiska termer. På grund av att skyddet för samförvarade handlingar alltid blir sämre bör samförvaring undvikas.

Om personerna inte är behöriga att ta del av samtliga hemliga handlingar i förvaringsutrymmet är det lämpligt att förvaringsutrymmet innehåller låsbara innerfack så att varje person kan tilldelas ett personligt innerfack (exempel 9:5). Samförvaring som innebär att personer delar på förvaringsutrymme utan inre indelning (t.ex. säkerhetsskåp med öppna hyllor) är olämpligt om personerna inte är behöriga att ta del av varandras handlingar och bör undvikas.

I de fall gemensam användning av hemliga handlingar (se avsnitt 9.15) används kan ett förvaringsutrymme utan låsbara innerfack användas för gruppens förvaring av de hemliga handlingarna.

Exempel 9:5

Flera personer använder gemensamt ett säkerhetsskåp med flera låsbara innerfack för förvaring av hemliga handlingar. Varje person har åtkomst till säkerhetsskåpet samt ett låsbart personligt innerfack i säkerhetsskåpet. Samförvaringsbeslut krävs då flera personer behöver åtkomst till förvaringsutrymmet (säkerhetsskåpet). Innerfacken är en indelning av säkerhetsskåpet men uppfyller inte kraven för den skyddsnivå som säkerhetsskåpet uppfyller varför samförvaringsbeslut krävs.

Endast de personer som samförvarar hemliga handlingar i förvaringsutrymmet får ges tillträde till förvaringsutrymmet. Det är lämpligt att på insidan av förvaringsutrymmet anslå en kopia av aktuellt samförvaringsbeslut. På så sätt underrättas de personer som förvarar handlingar i förvaringsutrymmet om vilka personer som är behöriga att få åtkomst till förvaringsutrymmet.

Om sammansättningen av personer som samförvarar hemliga handlingar ändras ska åtkomsten till förvaringsutrymmet ändras så att enbart de personer som samförvarar hemliga handlingar i förvaringsutrymmet har åtkomst till förvaringsutrymmet, t.ex. kan kod till säkerhetsskåp behöva bytas.

Det är inte lämpligt att på insidan av förvaringsutrymmet anslå vilka hemliga handlingar som samförvaras i förvaringsutrymmet.

Bilaga 3 innehåller en hänvisning till fastställd blankett för samförvaringsbeslut i Försvarsmakten.

Original av samförvaringsbeslut bör förvaras vid organisationsenhetens expedition eller motsvarande och ska arkiveras. Med anledning av de preskriptionstider som gäller för brott mot rikets säkerhet bör samförvaringsbeslut som omfattar hemliga handlingar i informationssäkerhetsklasserna HEMLIG/RESTRICTED, HEMLIG/CONFIDENTIAL och HEMLIG/SECRET sparas i 10 år och samförvaringsbeslut som omfattar hemliga handlingar i informationssäkerhetsklassen HEMLIG/TOP SECRET i 25 år. Riksarkivets tillstånd krävs för en eventuell gallring av samförvaringsbeslut.

9.12.2 Utrikesklassificerade handlingar

Samförvaring av utrikesklassificerade handlingar och materiel som innehåller utrikesklassificerade uppgifter ska i Försvarsmakten ske på samma sätt som för hemliga handlingar.[172]

172 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

9.12.3 Sekretessklassificerade handlingar

Om ett förvaringsutrymme ska användas gemensamt av flera personer för förvaring av sekretessklassificerade handlingar ska beslut om samförvaring inte fattas. I de fallen sekretessklassificerade handlingar ska användas gemensamt ska inte beslut om samförvaring eller gemensam användning fattas.[173] Sådana skyddsåtgärder är endast avsedda för hemliga och utrikesklassificerade handlingar. Det innebär dock inte att respektive person som samförvarar sekretessklassificerade handlingar därmed är behöriga att ta del av varandras sekretessklassificerade handlingar.

9.13 Medförande

Med medförande avses när en person i sin tjänsteutövning behöver transportera och förvara handlingar utanför en myndighets områden och lokaler (såväl allmänna handlingar som handlingar som inte är allmänna). Detsamma gäller för lagringsmedier som är avsedda för behandling av uppgifter i IT-system eller andra informationsbärare. Den hantering som arkiv- och expeditionspersonal utför vid distribution av handlingar och lagringsmedier är inte att betrakta som ett medförande.

9.13.1 Hemliga handlingar

> *Varje myndighet skall besluta i vilken omfattning hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre får medföras från myndighetens lokaler. Ett sådant beslut skall dokumenteras.*
>
> *Hemliga handlingar som medförs från myndigheten skall hållas under omedelbar uppsikt eller förvaras på ett sätt som motsvarar den skyddsnivå som gäller för förvaringen av handlingarna inom myndighetens lokaler.*
>
> 2 kap. 20 § Försvarsmaktens föreskrifter om säkerhetsskydd

Ett beslut bör dokumenteras i arbetsordning eller motsvarande.

Att hemliga handlingar som medförs från myndigheten ska hållas under uppsikt eller förvaras på ett sätt som motsvarar den skyddsnivå som gäller för förvaringen av handlingarna inom myndighetens lokaler gäller även handlingar som är placerad i informationssäkerhetsklassen HEMLIG/RESTRICTED.

En portfölj eller liknande som innehåller en hemlig handling får inte lämnas obevakad. Det är inte heller tillåtet att överlämna en hemlig handling till effektförvaring, t.ex. på järnvägsstationer eller hotell, även om effektförvaringen är bemannad.

173 Föreskrifter om samförvaring och gemensam användning saknas i 3 kap. Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Om det uppstår ett förvaringsbehov under en tjänsteresa inom riket, bör i första hand förvaringsmöjligheten hos ett militärt förband användas. Om detta inte är möjligt, kan polismyndigheten på orten vara ett alternativ.

Vid medförande av hemlig handling utanför myndighetens lokaler kan det vara lämpligt att förvara handlingen i förseglat emballage (kuvert eller säkerhetskuvert) så att eventuellt försök till intrång i emballaget kan uppmärksammas.

En hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre får medföras utanför Försvarsmaktens lokaler eller områden endast efter beslut av chefen för organisationsenheten, eller den han eller hon bestämmer, eller, såvitt avser Högkvarteret, lägst avdelningschef.

2 kap. 10 § första stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Syftet med föreskriften är att det i efterhand ska kunna vara möjligt att avgöra om en anställds medförande av en hemlig handling har varit tillåten. Föreskriften avser att motverka att anställda tar med sig hemliga handlingar där den anställdes arbetsuppgifter inte motiverar medförandet.

Huvudregeln är att hemliga handlingar inte ska tas med från ordinarie arbetsplats, då skyddet för en sådan handling alltid blir sämre. En verksamhets bedrivande kan dock innebära behov att medföra hemliga handlingar. En hemlig handling får medföras utanför Försvarsmaktens lokaler eller områden under den tid som krävs för att lösa de arbetsuppgifter för vilka den hemliga handlingen behövs. En hemlig handling bör normalt inte medföras utanför Försvarsmaktens lokaler eller områden under längre tid än en eller ett par dagar.

Ett beslut om medförande av hemlig handling krävs för såväl allmänna handlingar som handlingar som inte är allmänna (t.ex. arbetshandlingar som innehåller någon hemlig uppgift). Innan ett beslut om medförande av hemlig handling fattas bör den som fattar beslutet ta hänsyn till:

- För vilket ändamål den hemliga handlingen medförs och
- till vilka platser den hemliga handlingen ska medföras.

Ett beslut enligt föreskriften är en allmän handling och ska lämnas till expedition när den inte längre behövs. Besluten ska bevaras. Gallring ska ske om det finns ett gallringsbeslut som omfattar beslut om medförande av hemliga handlingar.

Med *Försvarsmaktens lokaler eller områden* avses alla vid organisationsenheten förekommande platser där hemliga handlingar behöver hanteras. Ett riktmärke kan vara sådana lokaler, byggnader och områden där organisationsenheten fattat beslut om tillträdesrätt.[174] I regel utgör lokaler, byggnader och områden som allmänheten inte har tillträde till en gräns, som om den passeras, innebär att ett medförande av hemlig handling kräver ett beslut om medförande (exempel 9:6). Vid ett fåtal organisationsenheter har dock allmänheten tillträde till område som disponeras av Försvarsmakten. Områden som allmänheten har tillträde till kan räknas in som myndighetens område om det huvudsakligen är Försvarsmakten som bedriver verksamhet i området (exempel 9:7).

Exempel 9:6

Högkvarteret är i Stockholm grupperat på flera skilda platser, bl.a. på Lidingövägen 24 och Banérgatan 62. En anställd som arbetar vid Lidingövägen 24 behöver till ett möte på Banérgatan 62 ta med sig en hemlig allmän handling samt en hemlig arbetshandling. Då de två hemliga handlingarna behöver föras ut från myndighetens lokaler (militärstabsbyggnaden på Lidingövägen 24) och området som omger myndighetens lokaler behöver den anställde lägst avdelningschefs beslut om medförande av de hemliga handlingarna.

Exempel 9:7

Vid Karlsborgs fästning finns flera militära verksamheter i olika byggnader inom fästningsområdet. Fästningsområdet är till stora delar öppet för allmänheten. Fästningsområdet är en del av myndighetens områden. För medförande av hemliga handlingar mellan de olika byggnaderna krävs inte att chef för organisationsenhet beslutar om medförande av hemlig handling.

Beslut om medförande av hemlig handling behöver inte fattas för varje hemlig handling som ska medföras. Ett beslut om medförande kan vara *generellt* och utformas för att gälla hela eller del av organisationsenheten, t.ex. för att omfatta personal inom angivna specifika verksamheter inom organisationsenheten (exempel 9:8). Om en organisationsenhet är uppdelad på flera geografiskt skilda platser där det kan antas att medförande i stor omfattning mellan platserna kommer att ske bör organisationsenhetens chef, eller den han eller hon bestämmer, fatta ett *generellt beslut om medfö-*

174 3 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd.

rande av hemliga handlingar. Formerna för beslut om medförande av hemlig handling anpassas då till verksamhetens behov.

Exempel 9:8

Juridiska staben i Högkvarteret är placerat på Banérgatan 62. Försvarsjuristerna har behov att regelbundet och med kort tids förvarning delta i möten på Lidingövägen 24. För att inte behöva fatta beslut i varje enskilt fall beslutar chefen för juridiska staben ett generellt beslut om medförande av hemliga handlingar. Beslutet dokumenteras i stabens arbetsordning och innebär att stabens personal får medföra hemliga handlingar mellan de platser i Stockholm där Högkvarteret är grupperat.

Det är lämpligt att det i arbetsordning eller motsvarande framgår vilka lokaler och områden vid organisationsenheten varifrån ett medförande av hemlig handling som kräver ett beslut om medförande. Av arbetsordning eller motsvarande är det också lämpligt att det framgår vem vid organisationsenheten som fattar beslutet och formerna för det.

Det är inte lämpligt att ett *generellt beslut om medförande av hemliga handlingar* tillåter regelmässigt medförande av hemliga handlingar till en anställds bostad. Det kan dock inte uteslutas att personal, t.ex. vissa ledamöter i Försvarsmaktens ledningsgrupp, är i behov av att regelbundet medföra hemliga handlingar till bostaden för genomläsning eller transport till kommande dags möten.[175] Ett regelmässigt medförande av hemliga handlingar till en anställds bostad kräver skyddsåtgärder i bostaden för förvaring och skydd mot obehörigas insyn.

Beslut enligt första stycket erfordras inte om det av något annat beslut följer att den hemliga handlingen ska medföras utanför en sådan lokal eller ett sådant område som avses i första stycket.

2 kap. 10 § andra stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Ett beslut om medförande behövs inte i det fall *det av ett annat beslut följer* att en hemlig handling får medföras. Detta kan t.ex. bestå av att en anställd muntligen ges arbetsuppgiften att delta i ett visst möte vid en annan myndighet eller delta i en militär övning, där hemliga uppgifter kommer att diskuteras, och den anställde för att kunna delta behöver medföra en viss hemlig handling (exempel 9:9 och exempel 9:10).

175 1 kap. 3 § andra stycket Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).

Exempel 9:9

Ola blir av sin chef beordrad att vid en annan myndighet delta i ett möte om försvarsplanering. För att kunna delta i mötet behöver Ola ta med sig en hemlig handling. Utan den hemliga handlingen är mötet meningslöst.

Något beslut om medförande av hemlig handling är inte nödvändigt att fatta då det av ordern följer att Ola får medföra hemliga handlingar till mötet. Chefens order om att delta i mötet är ett beslut som är tillräckligt för att Ola ska få ta med sig den hemliga handlingen.

Exempel 9:10

Zenobia, som arbetar på Högkvarteret i Stockholm, ska delta i ett projektmöte på Ledningsregementet i Enköping. Hon är osäker på vilka handlingar hon behöver ha med sig till mötet. Vissa hemliga handlingar skulle vara bra att ha med sig men det är inte nödvändigt för att kunna delta i mötet.

För de hemliga ”bra-att-ha-handlingarna” som inte är nödvändiga att ha med sig till mötet behöver Zenobia lägst avdelningschefs beslut om medförande av de hemliga handlingarna.

Detsamma gäller även ifråga om medförande av hemliga handlingar från ett militärt fartyg, luftfartyg eller från ett fordon, som befinner sig utanför en sådan lokal eller ett sådant område som avses i första stycket.

2 kap. 10 § tredje stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Medförande av hemlig handling från militärt fartyg, luftfartyg eller fordon kräver ett beslut om medförande om det militära fartyget, luftfartyget eller fordonet befinner sig utanför Försvarsmaktens lokaler eller områden. Detta avser de fall då en hemlig handling i huvudsak avses användas på fartyg, luftfartyg eller i fordon. Vid medförande av hemlig handling mellan två platser där transporten mellan platserna sker med ett militärt fartyg, luftfartyg eller fordon är inte avsikten att det ska krävas beslut om medförande av hemlig handling till och från det militära fartyget, luftfartyget eller fordonet. Ett beslut om medförande av hemliga handlingar mellan två platser innefattar de transportsätt som kommer till användning under medförandet.

En hemlig handling som har medförts utanför Försvarsmaktens lokaler eller områden ska snarast möjligt återföras eller överlämnas till den organisationsenhet som ska förvara handlingen.

2 kap. 11 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Närmaste chef för den person som medfört hemliga handlingar utanför Försvarsmaktens lokaler eller områden bör förvissa sig om att den hemliga handlingen är återförd eller överlämnad till den organisationsenhet som ska förvara den hemliga handlingen.

9.13.2 Utrikesklassificerade handlingar

Medförande av utrikesklassificerade handlingar och materiel som innehåller utrikesklassificerade uppgifter ska i Försvarsmakten ske på samma sätt som för hemliga handlingar.[176]

9.13.3 Sekretessklassificerade handlingar

Sekretessklassificerade handlingar som medförs från en organisationsenhet ska hållas under uppsikt eller förvaras på ett sätt som motsvarar de krav som gäller för förvaringen enligt 4 § i detta kapitel eller ett beslut enligt 5 § i detta kapitel.

3 kap. 6 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Det finns inget krav på att medförande av sekretessklassificerade handlingar ska beslutas av organisationsenheten.

Då det inte finns några föreskrifter som rör nycklar, kort och koder för förvaringsutrymmen som är avsedda för sekretessklassificerade handlingar får sekretessklassificerade handlingar som medförs förvaras i utrymmen som *inte* står under Försvarsmaktens kontroll, t.ex. effektförvaring. En lämpligare plats för förvaring bör dock väljas, om möjligt vid en myndighet eller organisationsenhet. Om en sekretessklassificerad handling medförs är det inte nödvändigt att handlingen under medförandet förvaras vid ett militärt förband eller polismyndighet.

176 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Vid förvaring av sekretessklassificerade handlingar i en bostad får handlingarna naturligtvis inte röjas för obehöriga och måste därför förvaras i ett förvaringsutrymme som uppfyller de krav som gäller för lägst skyddsnivå 1 om fler personer än innehavaren uppehåller sig i bostaden. Det är även möjligt att förvara en sekretessklassificerad handling i ett annat utrymme i bostaden som inte uppfyller krav för skyddsnivå 1 under förutsättning att motsvarande skyddsnivå kan upprätthållas och att organisationsenhet har fattat beslut om detta (avsnitt 9.11.8).

En portfölj eller dylik som innehåller en sekretessklassificerad handling får under medförande inte lämnas obevakad.

> *En sekretessklassificerad handling som har medförts utanför organisationsenhetens lokaler eller områden ska snarast möjligt återföras eller överlämnas till den organisationsenhet, myndighet eller annan som ska förvara handlingen.*
>
> 3 kap. 7 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Normalfallet är att sekretessklassificerade handlingar i Försvarsmakten ska förvaras i en organisationsenhets lokaler.

Medförande av sekretessklassificerade handlingar är begränsat till det behov som tjänsteutövningen kräver, t.ex. tillfälligt arbete utanför organisationsenhetens lokaler eller områden samt överlämning av sådana handlingar till en annan organisationsenhet eller myndighet. Sekretessklassificerade handlingar som har medförts får inte förvaras utanför den organisationsenhet eller den myndighet som ska förvara handlingarna. Det är således inte tillåtet att sekretessklassificerade handlingar medförs till t.ex. bostaden och förvaras där om det inte finns ett omedelbart behov av att ha handlingarna i bostaden för tjänsteutövningen.

Att medföra sekretessklassificerade handlingar och förvara handlingarna utanför organisationsenhetens lokaler eller områden för att handlingarna potentiellt skulle kunna behövas – d.v.s. utan koppling till den omedelbara tjänsteutövningens behov – är alltså inte tillåtet.

När tjänsteutövningen inte längre kräver att handlingarna medförs ska de snarast möjligt återföras. Om sekretessklassificerade handlingar medförs för att överlämnas till en annan organisationsenhet eller myndighet ska handlingarna snarast möjligt överlämnas. Med *annan* avses t.ex. att en sekretessklassificerad handling överlämnas till någon privat inrättning, t.ex. till ett företag som upphandlats av Försvarsmakten. Då det inte finns några föreskrifter som rör kvittering av sekretessklassificerade handlingar ska sådana handlingar ur säkerhetssynpunkt inte kvitteras då de överlämnas.

Det kan däremot av andra verksamhetsskäl finnas behov av kvittering vid överlämning av sådana handlingar.

Att sekretessklassificerade handlingar får medföras innebär normalt inte att de sekretessklassificerade uppgifterna i handlingarna får överlämnas till annan organisationsenhet, annan myndighet eller övriga.[177] Se även avsnitt 7.6-7.7 om behörigheter.

9.14 Medförandet utanför riket

9.14.1 Hemliga handlingar

Medförande av hemliga handlingar utomlands innebär vanligen att säkerhetsskyddet för handlingarna minskar. Då hemliga handlingar tas med på resor som t.ex. sker med reguljär flygtrafik kan handlingarna komma att uppmärksammas av andra staters personal i tull och säkerhetskontroller. En sådan möjlig uppmärksamhet utgör inte grund för att handlingarna inte ska märkas med sekretessmarkering och märkning med informationssäkerhetsklass. Hemliga handlingar som medförs utomlands av en anställd får inte placeras i bagage som checkas in, då förlorar den anställde kontrollen över handlingarna.

Medförande av hemliga handlingar underlättas ur säkerhetssynpunkt om det sker med militärt fartyg, luftfartyg eller fordon som disponeras av Försvarsmakten.

Något förbud mot att få medföra en kvalificerat hemlig handling utanför riket finns inte. Även sådana handlingar omfattas i Försvarsmakten av föreskriften nedan.

> *Hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre får medföras utanför riket endast efter beslut av chefen för organisationsenheten eller, såvitt avser Högkvarteret, lägst avdelningschef. Ett sådant beslut får fattas först efter skriftligt samråd med militära underrättelse- och säkerhetstjänsten i Högkvarteret.*
>
> *Beslut enligt första stycket erfordras inte om det av något annat beslut följer att hemliga handlingar ska medföras utanför riket eller överlämnas där.*
>
> 9 kap. 4 § första och andra styckena Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Föreskriften omfattar såväl allmänna handlingar som arbetshandlingar. Rätten att fatta ett beslut enligt föreskriften kan inte delegeras. Andra befattningshavare vid Högkvar-

177 8 kap. 1-3 §§ OSL.

teret, t.ex. stabschefer, omfattas inte av rätten att fatta ett beslut enligt föreskriften. Vid MUST är det säkerhetskontoret som svarar för samråd.

För en verksamhet som ska genomföras utomlands finns det normalt ett beslut om genomförandet. Ett sådant beslut är tillräckligt som grund för att få medföra hemliga handlingar om de krävs för att kunna genomföra verksamheten. Av beslutet om verksamhetens genomförande *följer* det att hemliga handlingar får medföras. I sådana fall behöver inte ett beslut enligt första stycket i föreskriften fattas. Det behöver inte av beslutet framgå vilka handlingar som ska medföras (exempel 9:11).

Exempel 9:11

F 17 ska med JAS 39 Gripen delta i en flygövning utomlands. För att kunna delta i övningen behöver F 17 använda flera IT-system för att planera och utvärdera flygningar. IT-systemen innehåller hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/SECRET. Dessutom behöver några hemliga skrivelser som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL användas under övningen.

För deltagandet finns ett beslut om att F 17 ska delta i övningen. Detta beslut är tillräckligt som grund för att få medföra de lagringsmedier som ingår i IT-systemen samt de hemliga skrivelserna. Något särskilt beslut eller samråd med MUST behöver således inte fattas eller genomföras.

Innan hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre medförs utanför riket ska chefen för organisationsenheten, eller den han eller hon bestämmer, upprätta en förteckning över handlingarna. I förteckningen ska anges om någon av handlingarna ska överlämnas utomlands. När det gäller de handlingar som ska återföras till riket ska chefen eller den han eller hon bestämmer, när handlingarna har återförts, kontrollera att dessa är desamma som de som enligt förteckningen ska återföras till riket.

9 kap. 4 § tredje stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Att få medföra en hemlig handling utomlands innebär inte att den hemliga handlingen får lämnas över till en annan stat eller mellanfolklig organisation. Medförandet innebär inte att uppgifter ur en sådan hemlig handling får delges genom visning eller muntligt för en företrädare för en annan stat eller mellanfolklig organisation. För att en hemlig handling ska få lämnas över eller uppgifter ur en sådan handling ska få delges

muntligt eller genom visning krävs att villkor om behörighet för personal vid utländsk myndighet är uppfyllda (avsnitt 7.7). Om villkoren inte är uppfyllda är ett överlämnande eller en delgivning inte tillåten.[178]

När hemliga handlingar har återförts till riket ska de kontrolleras mot förteckningen. Detta sker för att säkerställa att de hemliga handlingar som har medförts och som ska återföras verkligen har återförts. Om en handling inte kan återfinnas ska förhållandet säkerhetsrapporteras.[179]

Förteckningen är en allmän handling och ska lämnas till expedition när den inte längre behövs, t.ex. efter att kontroll av att de handlingar som har återförts till riket har genomförts. Förteckningen ska bevaras. Gallring ska ske om det finns ett gallringsbeslut som omfattar sådana förteckningar.

9.14.2 Utrikesklassificerade handlingar

Medförande av utrikesklassificerade handlingar och materiel som innehåller utrikesklassificerade uppgifter ska i Försvarsmakten ske på samma sätt som för hemliga handlingar.[180]

9.14.3 Sekretessklassificerade handlingar

Det finns ingen föreskrift om beslut att få medföra en sekretessklassificerad handling utomlands. För medförande av en sådan handling utanför riket ska 3 kap. 6-7 §§ Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar följas (avsnitt 9.13.3).

9.15 Gemensam användning

9.15.1 Hemliga handlingar

I Försvarsmakten förekommer verksamhet som innebär att flera personer har ett behov av att gemensamt använda hemliga handlingar. Det är i sådan verksamhet inte möjligt att låta varje person ha ett personligt exemplar av varje hemlig handling eller låta personerna kvittera de hemliga handlingarna mellan sig. Ett exempel på verksamhet där behov av gemensam användning av hemliga handlingar finns är ledningscentraler samt drift- och underhållsverksamhet i Försvarsmaktens anläggningar. Se även beskrivningen av principen för *öppen behörighetstilldelning* i avsnitt 7.10.

178 8 kap. 3 § OSL och 1 § förordningen om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet.
179 4 kap. 2 § Försvarsmaktens föreskrifter för Försvarsmaktens personal.
180 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Gemensam användning av hemliga handlingar utgår från att en *avgränsad* grupp av personer, givet verksamheten och personernas arbetsuppgifter, ska ges åtkomst till hemliga handlingar som är *gemensamma* för gruppen. Dessa hemliga handlingar är sådana som behövs för gruppens arbetsuppgifter. Varje person som ingår i en sådan grupp ska vara behörig att ta del av samtliga hemliga handlingar som är avsedda för gemensam användning. Personer som ingår i gruppen får *utan inbördes kvittenser* använda de hemliga handlingarna.

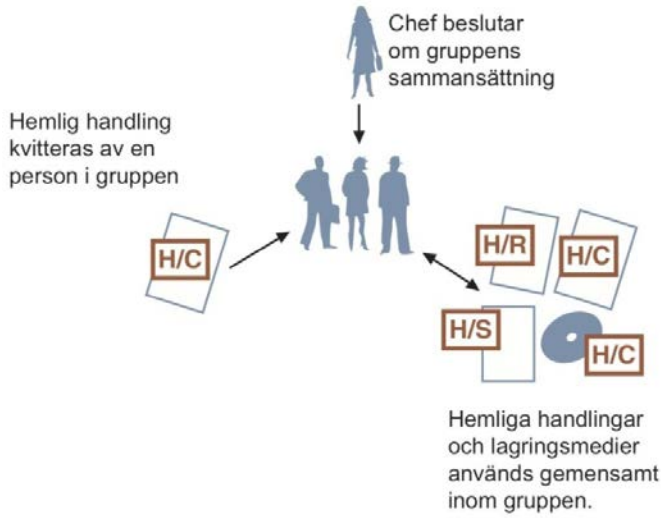


Bild 9:19 - Gemensam användning av hemliga handlingar.

Chef för organisationsenhet, eller den han eller hon bestämmer, får besluta vilka personer som får ingå i en grupp som gemensamt ska använda hemliga handlingar som förvaras hos enheten. Ett sådant beslut får endast fattas om det är oundgängligen nödvändigt för verksamheten. Ett beslut som avses i första meningen ska dokumenteras. Den som med stöd av ett sådant beslut har kvitterat mottagandet av en sådan handling ska, tillsammans med var och en av dem som ingår i gruppen, svara för att säkerhetsskyddet upprätthålls vid hantering av den hemliga handlingen.

Om någon som ska ingå i gruppen är anställd vid en annan organisationsenhet eller en annan myndighet ska chefen för den organisationsenhet som förvarar den hemliga handlingen, eller den han eller hon bestämmer, innan ett sådant beslut som avses i första stycket fattas samråda med berörd organisationsenhets säkerhetschef eller berörd myndighet.

2 kap. 8 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Grundregeln är att ett mottagande av en hemlig handling som är en allmän handling och som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre ska kvitteras av mottagaren.[181] Gemensam användning av hemliga handlingar ska därför tillämpas restriktivt och endast användas då det är oundgängligen nödvändigt med hänsyn till verksamheten och personernas avgränsade arbetsuppgifter. Gemensam användning av hemliga handlingar kan användas för handlingar som är placerade i informationssäkerhetsklasserna HEMLIG/RESTRICTED till och med HEMLIG/TOP SECRET, d.v.s. även för kvalificerat hemliga handlingar.

Rätten att fatta ett beslut enligt föreskriften får delegeras (exempel 9:12).

Ett beslut enligt föreskriften avser såväl när en person ska ingå i gruppen som när en person inte längre ska ingå i gruppen. Det är väsentligt att det för varje ändring av gruppens sammansättning finns en dokumenterad tidpunkt för ändringen. Bilaga 3 innehåller hänvisning till fastställd blankett för gemensam användning av hemliga handlingar samt samförvaring i Försvarsmakten.

Exempel 9:12

Chef för tredje ytstridsflottiljen får besluta att en fartygschef får fatta beslut om vilka personer som ska ingå i en grupp som gemensamt ska använda hemliga handlingar. En sådan grupp kan omfatta personal på fartyg som gemensamt behöver använda hemliga handlingar ombord på fartyget.

Det är lämpligt att varje grupp ges ett namn eller beteckning så att olika grupper kan åtskiljas. Det är också lämpligt att det i beslut om gemensam användning av hemliga handlingar framgår för vilket syfte gruppen inrättats.

Mottagandet av en hemlig handling som gemensamt ska användas av en grupp ska kvitteras av en person som ingår i gruppen. På kvittot bör det antecknas att den hemliga handlingen är avsedd för gemensam användning samt namn eller beteckning på gruppen för vilken handlingen är avsedd.

Det är lämpligt att det av anteckning på den hemliga handlingen, t.ex. genom en märkning, framgår att handlingen är avsedd för gemensam användning samt namn eller beteckning på gruppen för vilken handlingen är avsedd. På motsvarande sätt bör det i register där den hemliga handlingen är diarieförd även framgå att handlingen är avsedd för gemensam användning samt namn eller beteckning på gruppen för vilken handlingen är avsedd. Observera att anteckning på en hemlig handling som är avsedd för gemensam användning eller på handlingens kvitto inte är obligatorisk, men att det är en lämplig åtgärd. Användning av en sådan anteckning bör regleras i organisationsenhetens arbetsordning.

181 2 kap. 11 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Bild 9:20 - Exempel på märkning av hemlig handling som ska användas gemensamt.

När en hemlig handling inte längre är avsedd för gemensam användning bör en anteckning om gemensam användning överkorsas samt motsvarande ändring utföras i register där den hemliga handlingen är diarieförd.

Endast personer som ingår i en grupp får ges tillträde till ett förvaringsutrymme där hemliga handlingar som ska användas gemensamt förvaras. Ett sådant förvaringsutrymme kräver även samförvaringsbeslut då förvaringsutrymmet används gemensamt av flera personer.[182]

För tillträde till utrymme där förvaringsutrymmet är placerat ges spårbarhet i form av passerkontrollsystem eller besöksregistrering.[183] När en person inte längre ingår i en grupp ska personen inte längre ges tillträde till de förvaringsutrymmen där de hemliga handlingarna som ska användas gemensamt förvaras, t.ex. genom att byta kod till säkerhetsskåp.

Hemliga handlingar som är avsedda för gemensam användning ska inventeras på samma sätt som övriga hemliga handlingar. Vid muntlig delgivning eller genom

182 2 kap. 7 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
183 3 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd.

visning av uppgifter ur de hemliga handlingarna som ska användas gemensamt ska kvittering ske på delgivningskvitto eller delgivningslista. Dock ska inte personer som ingår i en grupp kvittera att de muntligen eller genom visning tagit del av uppgifter ur en hemlig handling som gemensamt ska användas av gruppen. Kvittering vid muntlig delgivning eller genom visning av sådana hemliga handlingar ska endast ske av personer som inte ingår i gruppen.

Det är lämpligt att det i arbetsordning eller motsvarande framgår hur gemensam användning av hemliga handlingar i övrigt ska tillämpas inom organisationsenheten. T.ex. vilka personer som genom lottning beslutar att en hemlig handling ska användas gemensamt av en grupp. I detta avseende är det inte lämpligt att personer i gruppen ska besluta om vilka handlingar som ska användas gemensamt.

Bestämmelsen om gemensam användning av hemliga handlingar gäller även för hemlig materiel och är även tillämplig i IT-system i fråga om lagringsmedier (exempel 9:13).[184] [185]

Exempel 9:13

För drift- och underhåll av t.ex. en telefonväxel som ska användas vid en stabsövning används ett lagringsmedium för konfiguration av telefonväxeln. Konfigurationen innehåller i detta exempel hemliga uppgifter i form av telefonnummer. Flera personer arbetar med drift- och underhåll av telefonväxeln och behöver då tillgång till lagringsmediet som innehåller konfigurationen.

Om någon som ingår i en sådan grupp som avses i 8 § detta kapitel uppmärksammar att en hemlig handling saknas, kan ha röjts eller obehörigen har ändrats, eller att säkerhetsskyddet av annan anledning kan antas brista, ska han eller hon omedelbart anmäla detta till den organisationsenhet som förvarar handlingen. Organisationsenheten ska därefter rapportera detta förhållande till den organisationsenhet eller myndighet som har upprättat handlingen. Om bristen kan hänföras till tillträdesbegränsningen ska även den organisationsenhet som svarar för denna underrättas.

2 kap. 9 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

184 1 kap. 3 § andra stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

185 7 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd.

All personal som ingår i en grupp för gemensam användning av hemliga handlingar svarar för att upprätthålla säkerhetsskyddet vid hantering av de hemliga handlingarna.

Var och en som får kännedom om säkerhetshotande verksamhet eller misstänker sådan verksamhet ska snarast möjligt rapportera förhållandet till sin närmaste chef, arbetsledare eller till säkerhetschef.[186] Om en hemlig handling som är avsedd för gemensam användning saknas, kan ha röjts eller obehörigen ha ändrats ska detta omedelbart rapporteras till den organisationsenhet som förvarar handlingen. Med *saknas* avses de fall där den hemliga handlingen konstaterats vara förkommen. Även andra förhållanden där säkerhetsskyddet kan antas brista ska omedelbart rapporteras till den organisationsenhet som förvarar handlingen.

I de fall en hemlig handling som är avsedd för gemensam användning saknas bör samtliga hemliga handlingar i förvaringsutrymmet, där den saknade handlingen förvaras, inventeras.

Beslut om gemensam användning av hemlig handling kan innehålla uppgifter som omfattas av sekretess enligt OSL. Uppgifter om vilka grupper som finns och vilka personer som ingår i grupperna kan t.ex. omfattas av sekretess. I vissa fall kan även uppgifter om platser och lokaler, för förvaring av de hemliga handlingarna som används gemensamt, omfattas av sekretess.

Gemensam användning av hemlig handling ersätter *Befintlighetsuppföljningssystem för hemliga handlingar* (BUSH). Begreppet BUSH ska inte längre användas. Skrivelserna [referens 49, 50 och 51] som är beslutade ska inte längre tillämpas i Försvarsmakten då regleringen i dessa äldre beslut har ersatts av 2 kap. 8-9 §§ Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

9.15.2 Utrikesklassificerade handlingar

Gemensam användning av utrikesklassificerade handlingar och materiel som innehåller utrikesklassificerade uppgifter ska i Försvarsmakten ske på samma sätt som för hemliga handlingar.[187]

9.15.3 Sekretessklassificerade handlingar

Beslut om gemensam användning ska inte fattas då sekretessklassificerade handlingar ska användas av flera personer.[188] Principen för *öppen behörighetstilldelning* (avsnitt 7.10) kan användas även för sekretessklassificerade handlingar.

186 4 kap. 2 § Försvarsmaktens föreskrifter för Försvarsmaktens personal.

187 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

188 Föreskrift om gemensam användning saknas i 3 kap. Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

9.16 Inventering

9.16.1 Hemliga handlingar

> ***Hemliga handlingar som är av synnerlig betydelse för rikets säkerhet skall inventeras minst en gång per år.***
>
> ***Andra hemliga handlingar skall inventeras i den omfattning som anges i föreskrifter enligt 45 §.***
>
> 9 § säkerhetsskyddsförordningen

Informationssäkerheten för hemliga uppgifter ska förebygga att sådana uppgifter röjs till obehöriga, oavsett om detta sker avsiktligt eller oavsiktligt. Inventering av hemliga handlingar är en skyddsåtgärd för att regelbundet kontrollera om handlingarna är i behåll eller om de har förlorats, t.ex. genom oaktsamhet.[189] Inventering av hemliga handlingar syftar även till att upprätthålla spårbarheten i hanteringen av hemliga handlingar som införts genom sändlistor, numrering av exemplar, registrering och kvittering vid mottagande. En positiv effekt av inventering av hemliga handlingar är att en innehavare av sådana handlingar anstränger sig för att behålla kontrollen över dessa.

En eventuell förlust upptäcks åtminstone senast vid ett inventeringstillfälle varvid undersökning med en menbedömning måste genomförs (kapitel 11). Med menbedömningen som underlag kan sedan åtgärder vidtas för att minimera eventuell skada.

Av erfarenhet ger varje inventeringstillfälle anledning till återlämnande av ett stort antal hemliga handlingar. En inventering motverkar därför att personal onödigtvis sparar hemliga handlingar som de inte längre behöver för arbetet.

Av föreskriften följer att en myndighet och en organisationsenhet i Försvarsmakten minst en gång per år även ska inventera kvalificerat hemliga handlingar som är *arkiverade*. Med per år avses att inventeringen ska genomföras en gång per kalenderår. Det finns inget krav om att tiden mellan två inventeringstillfällen måste vara mindre än ett år.

Inte endast pappershandlingar ska inventeras. En förlust av ett lagringsmedium innebär en förlust av potentiellt en mycket stor mängd hemliga uppgifter. Av 7 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd följer att även *lagringsmedier* som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre ska inventeras (se avsnitt 12.2.8). Även *handböcker*

189 Sidorna 74-75, Säkerhetsskydd prop. 1995/96:129.

och andra informationsbärare såsom *kartor* och *fotografier* som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre ska inventeras. Av 1 kap. 7 § Försvarsmaktens föreskrifter om säkerhetsskydd följer att även *materiel som innehåller hemliga uppgifter* som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre ska inventeras. Även *materiel vars existens är en hemlig uppgift* som är placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre ska inventeras.

Försvarsmakten rekommenderar att inventering av hemliga handlingar som är allmänna handlingar och som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre vid en myndighet genomförs en gång per år. Det kan även tilläggas att preskriptionstiden för brottet vårdslöshet med hemlig uppgift är två år.[190] Om inventering skulle göras med ett längre tidsintervall, skulle det få till följd att straffstadgandet förlorar betydelse genom att ett eventuellt brott hinner preskriberas. Försvarsmakten får inte för en annan myndighet föreskriva om inventeringens omfattning.[191] Istället ska en myndighet i interna föreskrifter om säkerhetsskydd ange inventeringens omfattning.[192]

I Försvarsmakten ska även andra hemliga handlingar som inte är kvalificerat hemliga men som har placerats i informationssäkerhetsklass HEMLIG/TOP SECRET inventeras en gång per år.[193]

Med inventering avses inte en sådan egenkontroll som en innehavare av hemliga handlingar kan göra för att förvissa sig om att de fortfarande är i behåll. Inte heller avses en sådan kontroll som en militär chef genomför före en verksamhet i syfte att kontrollera om personalen har med sig nödvändiga handlingar.

Underlag för att genomföra en inventering innehåller normalt uppgifter som omfattas av sekretess enligt OSL. Avsnitt 9.8.5 beskriver sekretess för sammanställningar över vem som förvarar hemliga handlingar och lagringsmedier.

> *Inventering av allmänna handlingar som är hemliga och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET liksom inventering av hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET skall protokollföras.*
>
> 2 kap. 21 § Försvarsmaktens föreskrifter om säkerhetsskydd

190 19 kap. 9 § brottsbalken.
191 44 § andra stycket säkerhetsskyddsförordningen.
192 9 § andra stycket säkerhetsskyddsförordningen.
193 2 kap. 12 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

Ett protokoll från en inventering av hemliga handlingar ska upprättas för *varje person* som har inventerats oavsett om några handlingar saknades eller inte. Om någon hemlig handling saknas ska protokollet innehålla uppgift om vilken handling som saknas.

Ett protokoll ska även upprättas efter inventering av kvalificerat hemliga handlingar och som är *arkiverade* vid en myndighet eller en organisationsenhet i Försvarsmakten. I Försvarsmakten ska ett sådant protokoll även omfatta andra hemliga handlingar som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET.

Efter att samtliga personer och arkiv vid en myndighet, eller organisationsenhet i Försvarsmakten, har inventerats bör ett *samlat inventeringsprotokoll* upprättas som sammanfattar resultatet av inventeringen. Av protokollet kan t.ex. framgå att hemliga handlingar vid myndigheten, eller organisationsenheten, har inventerats och att inga handlingar saknades. Då det p.g.a. sjukdom och andra omständigheter ibland inte är möjligt att inventera alla personer bör det av ett sådant samlat inventeringsprotokoll framgå vilka personer som inte har inventerats. Det samlade inventeringsprotokollet bör distribueras till myndighetens säkerhetsorganisation och till närmaste chef för de personer som inte har inventerats. Så snart en person, som inte har fått sina hemliga handlingar inventerade, återkommer måste närmsta chef se till att den anställde får inventerat sina hemliga handlingar.

Om det samlade inventeringsprotokollet visar på fel eller brister i säkerhetsskyddet, vid en myndighet eller organisationsenhet i Försvarsmakten, som inte endast är av ringa betydelse ska detta anmälas till Försvarsmaktens säkerhetsskyddschef.[194] [195]

Det är lämpligt att alla protokoll från inventering av hemliga handlingar sparas vid en expedition eller motsvarande. Protokollen ska kunna visas upp vid tillsyn av säkerhetsskyddet. Inventeringsprotokoll vid myndigheter under försvarsdepartementet ska bevaras, de får inte gallras.[196]

I Försvarsmakten ska förhållandet att en hemlig handling saknas rapporteras. En sådan rapport ska vidarebefordras till MUST.[197] Expeditionspersonalen får även rapportera ett sådant förhållande till MUST, t.ex. om förhållandet gäller personer vid organisationsenhetens säkerhetsorganisation eller då organisationsenhetens säkerhetsorganisation inte vidtar någon åtgärd trots tidigare rapportering.

194 1 kap. 8 § Försvarsmaktens föreskrifter om säkerhetsskydd.

195 1 kap. 6 § första stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

196 2 § Riksarkivets föreskrifter om gallring av handlingar rörande hanteringen av hemliga och kvalificerat hemliga handlingar hos myndigheter under Försvarsdepartementet.

197 1 kap. 6 § andra stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

Organisationsenhetens bestånd av allmänna hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET och som inte är arkiverade ska inventeras en gång per år.

2 kap. 13 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

I Försvarsmakten är det hemliga handlingar som är allmänna handlingar och som har placerats i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre som ska inventeras. Hemliga handlingar som har placerats i informationssäkerhetsklass HEMLIG/RESTRICTED ska inte inventeras då krav på registrering av exemplar inte finns för sådana handlingar.

I Försvarsmakten ska även handlingar och lagringsmedier som *används gemensamt* av flera personer inventeras (avsnitt 9.15).

Inventering av hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET ska utföras av två inventeringsförrättare.

2 kap. 14 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Det är självklart att ingen av dem får vara den person som ska få sina hemliga handlingar inventerade. I fråga om handlingar som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET och som har arkiverats bör inventeringen inte endast utföras av personal som arbetar med arkivtjänst. Personal från expedition kan delta under förutsättning att det är fråga om personer som där arbetar med registrering av sådana handlingar. Även en säkerhetschef eller en annan person ur den militära säkerhetstjänsten kan vara lämplig att utföra inventering i arkiv av hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET.

Att en person genomför inventering innebär inte att personen är behörig att ta del av uppgifterna i handlingarna. Även om personerna som genomför inventeringen inte ska ta del av uppgifterna i handlingarna är det ofrånkomligt att detta kan ske under ett inventeringstillfälle. Personal som genomför inventeringen ska därför i övrigt ha till arbetsuppgift att hantera hemliga uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/TOP SECRET. Personerna som genomför inventeringen behöver inte kvittera att de genom visning har delgivits uppgifter ur handlingarna (avsnitt 9.10). Uppgift om vilka personer som har genomfört inventeringen framgår på inventeringsprotokollet.

Det är inte lämpligt att Försvarsmaktens handlingar som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET hanteras av tillfälligt inhyrd personal från bemanningsföretag eller liknande så att de skulle kunna ta del av uppgifterna i handlingarna. De personer som genomför inventeringen bör därför vara försvarsmaktsanställda, på motsvarande sätt som att förstöring av sådana handlingar skriftligen ska intygas av två försvarsmaktsanställda.[198]

> *Varje organisationsenhet ska besluta hur hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre ska inventeras.*
>
> 2 kap. 15 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Det är lämpligt att det i arbetsordning eller motsvarande framgår hur en inventering ska genomföras. Av beslutet ska även framgå hur lagringsmedier ska inventeras. Inventering av hemliga handlingar som inte är arkiverade kan ske i ett uttalat linjeansvar långt ner i organisationen. Detta medför att inventeringen kommer att gå fort och inte särskilt behöver belasta expeditionspersonal. En årlig inventering kommer att reducera de kostnader som en eftersökning av äldre, förkomna hemliga handlingar annars hade kunnat komma att medföra.

En inventering av hemliga handlingar och lagringsmedier utgår vanligtvis från en förteckning per person med en sammanställning av de handlingar och lagringsmedier som har registrerats på den personen (s.k. inventeringslista). En inventering av en hemlig handling syftar till att fastställa om handlingen är i behåll eller har förkommit. Det är därför oftast tillräckligt att jämföra handlingens unika dokumentbeteckning och exemplarnummer på handlingens första sida med motsvarande uppgift i inventeringslistan.

I det fall en handling består av flera lösa bilagor eller lagringsmedier måste även dessa kontrolleras. Om handlingen har gått sönder, t.ex. då sidor lossnat, bör en noggrannare kontroll av att handlingen är intakt ske. Att räkna varje sida i en hemlig handling, inklusive bilagor, bör endast ske då det finns tydliga indikationer på att handlingen inte är intakt. I detta avseende bör noggrannheten i inventeringen vara större för handlingar som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET.

I böcker som består av lösbladssystem, samt i ohäftade handlingar, bör varje blad kontrolleras.

198 2 kap. 17 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

Handlingar som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET och som förvaras i en förseglad låda i ett arkiv kan inventeras genom att kontrollera att lådan är i behåll, samt att lådan och förseglingen är intakt. En sådan försegling måste dock vara av en sådan typ att det ska kunna upptäckas om den ursprungliga förseglingen har ersatts med en ny. Det är också nödvändigt att förteckningar över innehållet i en sådan låda hålls aktuella vid en expedition. Det kan t.ex. i det register där en handling är diarieförd framgå i vilken låda handlingen är placerad. När en sådan låda iordningsställs bör två personer delta i arbetet, inklusive förseglingen av lådan och registrering av handlingarna.

Allmänna handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre och som används i en internationell militär insats ska, om möjligt, inventeras vid avlösning (rotation) och i övrigt när det finns särskild anledning.

Allmänna hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre och som används i övrig verksamhet enligt 1 § i detta kapitel ska, om möjligt, inventeras när verksamheten avlutas, dock minst en gång varje år, och i övrigt när det finns särskild anledning.

9 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

När Försvarsmakten deltar i en internationell militär insats behöver inventering av hemliga handlingar genomföras oftare med hänsyn till att personalen byts ut med en regelbundenhet på 6-9 månader. Med om möjligt avser t.ex. om personalsituationen medger att inventering kan ske.

Övrig verksamhet enligt 1 § avser när Försvarsmakten deltar i internationell fredsfrämjande verksamhet eller annat internationellt samarbete samt i utbildning eller förberedelser för sådan verksamhet eller samarbete, och deltagande utomlands i förevisningar av materiel eller verksamhet.[199]

9.16.2 Utrikesklassificerade handlingar

Inventering av utrikesklassificerade handlingar och materiel som innehåller utrikesklassificerade uppgifter ska i Försvarsmakten genomföras på samma sätt som för hemliga handlingar.[200]

199 9 kap. 1 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
200 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

9.16.3 Sekretessklassificerade handlingar

Sekretessklassificerade handlingar ska inte inventeras i Försvarsmakten då några krav på spårbarhet eller att förlust av sådana handlingar ska upptäckas inte finns.[201]

9.17 Kopiering och utdrag

9.17.1 Hemliga handlingar

> *Varje myndighet skall besluta vilka rutiner som skall tillämpas i samband med kopiering av eller utdrag ur en hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre. Beslutet skall dokumenteras.*
>
> *Kopia av eller utdrag ur en hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET får göras endast efter medgivande av myndighetens chef eller den han bestämmer.*
>
> 2 kap. 9 § Försvarsmaktens föreskrifter om säkerhetsskydd

För en myndighet är det lämpligt att rutinerna anges i myndighetens interna föreskrifter om säkerhetsskydd.[202] För en organisationsenhet i Försvarsmakten är det lämpligt att det i arbetsordning framgår vilka rutiner som gäller. Rutinerna kan vara olika för en hemlig handling som är en allmän handling eller inte är en allmän handling (en s.k. arbetshandling).

Rutinerna ska förebygga att s.k. *svartkopior* uppstår. Svartkopior är oregistrerade kopior av eller utdrag ur hemliga handlingar som ska registreras. Svartkopior minskar skyddseffekten av att hanteringen av övriga exemplar är spårbar. Om svartkopior förekommer i en verksamhet underlättar det även för personer, som är behöriga till uppgifterna i handlingarna, att kopiera eller avbilda handlingarna i syfte att gå främmande makt tillhanda. En förlust av en svartkopia kan inte uppmärksammas i en inventering av hemliga handlingar då uppgift om kopian (exemplaret) saknas i registret över myndighetens hemliga handlingar. Svartkopior får därför naturligtvis inte förekomma i verksamheten. Rutinerna om kopiering och utdrag har därför en stark koppling till krav på registrering och exemplarhantering (avsnitt 9.8.4).

I fråga om hemliga handlingar som är allmänna handlingar och som har placerats i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre bör rutinerna utformas så att kopiering eller utdrag endast får genomföras på uppdrag av den funk-

201 Föreskrift om inventering saknas i 3 kap. Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

202 45 § säkerhetsskyddsförordningen.

tion vid myndigheten som svarar för registrering av de hemliga handlingarna (expedition eller motsvarande). På detta sätt säkerställs att kopiorna och utdragen registreras.

En rutin som också är godtagbar ur säkerhetssynpunkt är att den person, som utarbetar en hemlig handling som är en allmän handling och som är placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre, skriver ut eller kopierar handlingen i det antalet exemplar som handlingen ska distribueras i. Originalet och kopiorna måste lämnas till den funktion vid myndigheten som svarar för registrering av hemliga handlingar. Funktionen ser till att de nya exemplaren registreras, förses med kvitton och sedan att de distribueras.

Det måste av de dokumenterade rutinerna även framgå vem som beslutar om att kopiering eller utdrag ska få genomföras. Ett sådant beslut fattas självständigt inom en myndighet eller i Försvarsmakten inom en organisationsenhet. Det finns inget krav på att ett sådant beslut ska föregås av samverkan för en handling som har upprättats av en annan myndighet eller i Försvarsmakten av en annan organisationsenhet. En lämplig ordning är att en chef i den verksamhet där handlingen *förvaras* beslutar om kopiering eller utdrag. Det är således inte nödvändigt att det ska vara en chef för den verksamhet som har *upprättat* handlingen som ska besluta om kopiering eller utdrag. Den chef som har fattat beslut om fördelning av ärenden i en verksamhet bör även få fatta beslut om kopiering eller utdrag. Beslut om kopiering kan således ske nära den verksamhet som har behov av flera kopior, t.ex. om flera personer ska arbeta tillsammans och varje person behöver ett eget exemplar av en viss handling. Med detta synsätt motverkas förekomsten av svartkopior samtidigt som spårbarheten ökar och tillgängligheten till informationstillgångar underlättas.

För *arkiverade handlingar*, där inte exemplar i övrigt finns, är det lämpligt att en chef för den verksamhet som handlingen rör fattar beslut om kopiering eller utdrag (kan jämföras med att upprättaren av en handling även skriver sändlistan för handlingen). Om verksamheten har lagts ner och inte kan sägas motsvaras av någon befintlig verksamhet bör chef för den verksamhet som är i behov av en kopia eller ett utdrag få fatta beslut om kopiering eller utdrag.

Ett beslut om att kopiering eller utdrag får ske (vanligen kallat *kopieringstillstånd*) grundas på de villkor som gäller för behörighet att ta del av hemliga uppgifter (avsnitt 7). I de fall villkoren om behörighet inte är uppfyllda får inte kopiering eller utdrag ske. Det är lämpligt att det av ett beslut framgår för vilket ändamål som kopieringen eller utdraget avser och vem som ska ta emot kopian eller utdraget.

Krav på beslut om kopiering och utdrag gäller även då en begäran om utlämnande av allmän handling ska hanteras, t.ex. då det behövs en kopia för att bedöma om en allmän handling som är hemlig och som har placerats i informationssäkerhetsklass

HEMLIG/CONFIDENTIAL eller högre kan lämnas ut helt eller delvis. Rutinerna måste därför utformas så att kravet på skyndsamhet enligt 2 kap. 12 § TF tillgodoses.

Kravet på beslut om kopiering eller utdrag ur en handling som är placerad i informationssäkerhetsklass HEMLIG/TOP SECRET gäller även för handlingar som inte är allmänna (arbetshandlingar). I Försvarsmakten är det chef för en organisationsenhet, eller den han eller hon bestämmer, som ska fatta beslut om kopiering eller utdrag ur en handling som är placerad i informationssäkerhetsklass HEMLIG/TOP SECRET.[203]

> *Har en kopia av eller ett utdrag ur en allmän handling som är hemlig och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre gjorts, skall uppgift om detta liksom uppgift om till vem kopian eller utdraget har lämnats antecknas i register eller liggare.*
>
> *Om det inte framgår av ett utdrag ur en allmän handling som är hemlig och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre till vilken handling utdraget hör, skall det på utdraget antecknas från vilken handling utdraget har gjorts.*
>
> 2 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd

Syftet med åtgärderna är att säkerställa spårbarheten i hanteringen av hemliga handlingar som är allmänna handlingar och som har placerats i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre. En kopia eller ett utdrag ur en sådan hemlig handling ska hanteras så att spårbarhet finns för kopians eller utdragets livscykel, d.v.s. spårbar hantering inklusive inventering till dess att en kopia eller utdrag har förstörts.

Åtgärderna har inte setts nödvändiga för hemliga handlingar som inte är allmänna handlingar. Detta underlättar arbetet med att ta fram en hemlig handling.

9.17.2 Utrikesklassificerade handlingar

Kopiering eller utdrag ur utrikesklassificerade handlingar ska i Försvarsmakten ske på samma sätt som för hemliga handlingar.[204]

9.17.3 Sekretessklassificerade handlingar

Det finns inga krav i Försvarsmakten på rutiner för hur sekretessklassificerade handlingar ska kopieras eller hur utdrag ska ske ur sådana handlingar. En organisationsen-

203 1 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
204 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

het ska inte fatta några särskilda beslut om vilka rutiner som gäller för sekretessklassificerade handlingar som kan begränsa hanteringen av handlingarna.[205]

Sekretessklassificerade handlingar får kopieras och utdrag får göras ur sådana handlingar om det är nödvändigt för arbetet, t.ex. av den person som innehar en sådan handling. Uppgift om kopia eller utdrag ur en sekretessklassificerad handling ska inte antecknas i ett register eller motsvarande. Det finns således inga krav på spårbarhet för en sådan handling.

9.17.4 Utskrifter ur IT-system

Det är vanligt att informationstillgångar skapas i IT-system. I IT-system behandlas elektroniska handlingar. Även andra upptagningar kan behandlas i IT-system, t.ex. i form av video eller ljud.

När en hemlig handling skrivs ut i ett IT-system uppstår i pappersform en kopia av eller ett utdrag ur den hemliga handlingen. Sådana kopior och utdrag ska omfattas av samma skydd som övriga hemliga handlingar. Är det fråga om en kopia av eller utdrag ur en hemlig handling som är en allmän handling och som har placerats i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre uppstår ett *nytt exemplar* som ska registreras.[206] Registreringen är nödvändig för att upprätthålla spårbarheten i hanteringen av kopian eller utdraget, till dess att kopian eller utdraget har förstörts. Om inte en sådan kopia eller utdrag registreras är det fråga om en s.k. svartkopia (exempel 9:14).

Exempel 9:14

Henrik arbetar med förnödenhetsförsörjning. Han har i ett IT-system, som är godkänt för behandling av hemliga uppgifter, tagit emot en hemlig rapport om materielstatus från en annan myndighet. Rapporten är en allmän handling som är placerad i informationssäkerhetsklass HEMLIG/SECRET. Henrik skriver ut rapporten på en skrivare som finns i IT-systemet för att lättare kunna läsa den.

Då Henrik inte registrerar utskriften är den utskriva handlingen en svartkopia. Utskriften kommer inte att kunna uppmärksammas i en inventering och en eventuell förlust av handlingen går obemärkt förbi.

205 Föreskrift om kopiering och utdrag saknas i 3 kap. Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

206 2 kap. 19 § Försvarsmaktens föreskrifter om säkerhetsskydd.

En hemlig uppgift i ett IT-system ska ha ett säkerhetsskydd som motsvarar det säkerhetsskydd som uppgiften har placerats i.[207] En vägledning för hur en myndighet ska se på utskrifter av hemliga handlingar i ett IT-system är de rutiner som ska finnas vid myndigheten om kopiering av eller utdrag ur en hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre (avsnitt 9.17.1). Skyddsåtgärderna för utskrifter i ett IT-system kan inte vara mindre långtgående än skyddsåtgärderna för kopiering av eller utdrag ur andra hemliga handlingar.

När ett IT-system innehåller register eller databaser är det viktigt att uppmärksamma att ett utdrag ur en databas blir en allmän handling.

Exempel 9:15

Juhani ska delta i ett arbetsmöte om materiel som är placerade i flera förråd. Till mötet behöver han ha med sig underlag ur en databas. Juhani genomför en sökning i databasen. Underlaget innehåller uppgifter som omfattas av sekretess enligt 15 kap. 2 § OSL och är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL. Resultatet av sökningen presenteras i form av en PDF-fil. PDF-filen består av ett fixerat innehåll som nått sin slutgiltiga form och är en färdig elektronisk handling. PDF-filen utgör en allmän handling och ska registreras. I det fall PDF-filen skrivs ut ska exemplaret registreras och ges samma säkerhetsskydd som andra hemliga handlingar som är allmänna handlingar.

Inför utveckling av ett IT-system, som är avsett för behandling av hemliga uppgifter, måste frågan om utskrifter uppmärksammas i IT-systemets säkerhetsmålsättning i form av *tillkommande säkerhetskrav* (avsnitt 13.3).[208] Det kan i fråga om utskrifter i IT-system finnas motstridiga krav vad gäller önskvärd användarfunktionalitet och krav på skydd.

En lämplig ordning kan vara att utskrifter i ett IT-system centraliseras vid en funktion, t.ex. en expedition, där handlingarna registreras och användaren kvitterar ut handlingen. En annan ordning kan vara att ett IT-system genom tekniska funktioner tillåter att användarna skriver ut arbetshandlingar men inte allmänna handlingar.

207 7 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd.
208 7 kap. 7 § Försvarsmaktens föreskrifter om säkerhetsskydd och 4 kap. 1 och 3 §§ Försvarsmaktens interna bestämmelser om IT-säkerhet.

9.17.5 Kopieringsmaskiner

Anskaffning och användning av en digital kopiator får i Försvarsmakten först ske efter auktorisation.[209] En digital kopiator är ett IT-system där stora mängder uppgifter behandlas. Om ett sådant IT-system är avsett för kopiering av uppgifter som är placerade i informationssäkerhetsklass ska det finnas ett säkerhetsskydd för uppgifterna. Skyddet kan bl.a. bestå av att det ska finnas i förväg dokumenterade rutiner för hur underhåll och service ska genomföras. Skydd mot röjande signaler och hur kopiatorn ska skyddas mot manipulation är andra frågor som måste uppmärksammas i auktorisation.

MUST har uttryckt sin uppfattning om kopieringsmaskiner [referens 1].

En kopiator bör förses med en tydlig märkning som visar vilka slag av uppgifter som kopiatorn är avsedd för (bild 9:21). Märkningen ska förebygga att personer som ska använda en kopiator inte av misstag använder den för uppgifter som kopiatorn inte är avsedd för.

Bild 9:21 - Exempel på märkning av en kopiator.

Följande ska beaktas vid användning av en kopieringsmaskin i Försvarsmakten:

- Att original inte lämnas kvar, både under lock och i eventuella matningsfack.
- Att alla kopior blir utskrivna och att inga kopior lämnas kvar i utmatningsfack.
- Att alla kopior tas omhand vid papperstrassel.
- Att eventuella arbetsminnen töms på information genom att göra dem spänningslösa genom att stänga av kopiatorn eller med för ändamålet avsedd funktion.

209 6 § Försvarsmaktens interna bestämmelser om IT-verksamhet.

Exakt tillvägagångssätt kan vara individuellt beroende på typ av kopieringsmaskin och bör då framgå på maskinen.

- En kvarglömd sekretessbelagd handling som hittas i kopieringsmaskinen ska lämnas till säkerhetschefen.
- Service som utförs av person som inte är försvarsmaktsanställd ska övervakas.

Ett fast eller löstagbart lagringsmedium (t.ex. en hårddisk) som ingår i en kopiator får i Försvarsmakten inte överlämnas till någon annan för användning eller försäljning. Lagringsmedium måste monteras ut ur kopiatorn innan kopiatorn återlämnas eller kasseras.

9.17.6 Kopiering för utlämnande av allmän handling

Om en allmän handling förvaras vid en myndighet som en elektronisk handling eller som en annan upptagning i ett IT-system är myndigheten inte skyldig att lämna ut den allmänna handlingen i elektronisk form, om inte annat följer av en lag. Det är tillräckligt att normalt lämna ut en allmän handling i pappersform.[210] Tekniska möjligheter att sammanställa och analysera digital information medför att Försvarsmaktens informationstillgångar som genom utlämnande har gjorts tillgängliga för allmänheten kan användas för att finna hemliga uppgifter. Genom att kombinera flera uppgifter (aggregation) erhålls *nya uppgifter* som inte hade varit möjlig att erhålla med tillgång endast till uppgifterna var och en för sig.[211]

En organisationsenhet i Försvarsmakten bör vid en eventuell utlämning av en allmän handling, efter genomförd sekretessprövning, överväga att endast lämna ut handlingen i pappersform eller genom telefax. Det kan dock finnas handlingar som om de sprids till allmänheten i elektronisk form gynnar Försvarsmaktens verksamhet, t.ex. broschyrer, redovisningar och handböcker. Handlingar i elektronisk form sprids till allmänheten bl.a. genom Försvarsmaktens webbplats. I fråga om handlingar som ska användas av uppdragstagare (t.ex. konsulter) eller handlingar som sänds till andra myndigheter är det vanligtvis lämpligt att handlingarna distribueras i elektronisk form.

9.18 Återlämning

Återlämning av handlingar och lagringsmedier bör vara en naturlig del i en rutin för avslutad anställning eller byte av tjänst inom en myndighet.

I internationella samarbeten där utländsk personal tjänstgör vid svenska enheter bör särskilt den utländska personalens återlämning av handlingar uppmärksammas.

210 2 kap. 13 § TF
211 Avsnitt 4.3.4 i H Säk Sekrbed A.

9.18.1 Hemliga handlingar

En hemlig handling som är en allmän handling och som är placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre ska återlämnas om den inte längre behövs av den anställde för sitt arbete. Återlämning sker normalt till en expedition, där den tas om hand för arkivering eller förstöring. Då en sådan handling lämnas tillbaka är det lämpligt att originalkvittot återlämnas till mottagaren, eftersom det är det enda han eller hon har för att bevisa att den hemliga handlingen är återlämnad.

Det finns inget krav ur säkerhetssynpunkt på återlämning av en hemlig handling som är placerad i informationssäkerhetsklass HEMLIG/RESTRICTED. En sådan handling som är en allmän handling ska dock *originalet* återlämnas för bevarande till en expedition eller motsvarande då den inte längre behövs. En kopia av en sådan handling får lämnas till en expedition för förstöring eller förstöras av innehavaren.

Vid återlämning av en hemlig handling, som är en allmän handling och som är placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre, är det nödvändigt att den som tar emot handlingen bedömer om handlingen är intakt. I det fall handlingen består av flera lösa bilagor eller lagringsmedier måste även dessa undersökas i samband med återlämningen. Om handlingen har gått sönder, t.ex. då sidor lossnat, bör en noggrannare kontroll genomföras. Att räkna varje sida i en hemlig handling, inklusive bilagor, bör endast ske då det finns tydliga indikationer på att handlingen inte är intakt. I detta avseende bör noggrannheten vara större för handlingar som har placerats i informationssäkerhetsklass HEMLIG/TOP SECRET.

Om en bok som består av lösbladssystem återlämnas bör varje blad kontrolleras.

Om delar av en återlämnad handling saknas ska händelsen säkerhetsrapporteras.[212]

Om det vid en organisationsenhet är känt att en tidigare anställd inte har återlämnat sådana hemliga handlingar som ska återlämnas ska det inträffade säkerhetsrapporteras.[213] Det finns i sådana fall ingen anledning att vänta till den årliga inventeringen för att i samband med den upptäcka det inträffade.

9.18.2 Utrikesklassificerade handlingar

Återlämning av utrikesklassificerade handlingar ska i Försvarsmakten ske på samma sätt som för hemliga handlingar.[214]

212 4 kap. 2 § Försvarsmaktens föreskrifter för Försvarsmaktens personal.
213 4 kap. 2 § Försvarsmaktens föreskrifter för Försvarsmaktens personal.
214 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

9.18.3 Sekretessklassificerade handlingar

Det finns inget krav ur säkerhetssynpunkt på återlämning av en sekretessklassificerad handling som inte längre behövs. Endast en sekretessklassificerad handling som är en allmän handling i original ska återlämnas för bevarande till en expedition eller motsvarande då den inte längre behövs. En kopia av en sekretessklassificerad handling får lämnas till en expedition för förstöring eller förstöras av innehavaren.

9.19 Förstöring

9.19.1 Hemliga handlingar

> *Förstöring av hemliga handlingar eller av materiel som innehåller hemliga uppgifter skall ske så att åtkomst och återskapande av uppgifterna omöjliggörs.*
>
> *Förstöring av sådana hemliga handlingar och sådan materiel som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre skall dokumenteras utom såvitt avser karbonpapper, karbonband och färgband.*
>
> 2 kap. 22 § Försvarsmaktens föreskrifter om säkerhetsskydd

En myndighet bör i interna föreskrifter om säkerhetsskydd[215] meddela vilka krav som gäller för förstöring av hemliga handlingar och materiel vid myndigheten. Sådana interna föreskrifter ska säkerställa att förstöringen uppfyller 2 kap. 22 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Föreskriften gäller alla former av handlingar såväl hemliga handlingar som är allmänna handlingar som hemliga handlingar som inte är allmänna, t.ex. arbetshandlingar som skickas i samrådssyfte eller personliga utkast och minnesanteckningar. Även t.ex. kartor, handböcker och fotografier är handlingar som omfattas av föreskriften om de innehåller någon hemlig uppgift.

En hemlig handling eller materiel som innehåller hemliga uppgifter ska intill dess att förstöringen är genomförd förvaras enligt de föreskrifter som gäller för den informationssäkerhetsklass som handlingen eller materielen är placerad i (se avsnitt 9.11.1).

Även formerna för förstöringen måste utformas så att obehörigas åtkomst till handlingarna och materielen är omöjliggjort.

215 45 § säkerhetsskyddsförordningen.

Hur förstöringen sker är upp till en myndighet att avgöra. Förstöring kan t.ex. ske genom mekanisk bearbetning (dokumentförstörare etc.) och bränning.

Förstöring av hemliga handlingar och materiel som innehåller hemliga uppgifter får utföras genom en upphandlad tjänst. En sådan tjänst kan dock inte komma i fråga utanför Sverige då det skulle vara omöjligt att säkerställa säkerhetsskyddet.

Det normala är att en hemlig handling förstörs av expeditionspersonalen efter det att den har återlämnats och då sker dokumentationen med automatik. Om en handling, som får förstöras, förstörs av någon enskild så ska rutinen vara att registervårdande enhet omedelbart meddelas om vidtagen åtgärd så att en anteckning om att den hemliga handlingen är förstörd kan göras i det register där den är diarieförd (se avsnitt 9.8.4).

Hemliga handlingar som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET förekommer normalt i liten omfattning. Det är därför lämpligt att dokumentera förstöringen direkt efter att förstöringen har ägt rum. Om omfattningen av sådana handlingar är liten bör förstöringen genomföras lokalt, t.ex. i dokumentförstörare vid expedition eller motsvarande, även om en upphandlad tjänst för förstöring av hemliga handlingar används.

Kravet på att förstöringen ska dokumenteras gäller även en hemlig handling som inte är en allmän handling.

Riksarkivet har meddelat föreskrifter om gallring som innebär att förstöringsrapporter över hemliga handlingar ska gallras efter 10 år och förstöringsrapporter över kvalificerat hemliga handlingar ska gallras efter 25 år.[216] Föreskrifterna om sådan gallring gäller för myndigheter under försvarsdepartementet.

> *För gallring av hemliga handlingar gäller särskilda bestämmelser som meddelas av Riksarkivet.*
>
> 2 kap. 23 § Försvarsmaktens föreskrifter om säkerhetsskydd

Föreskriften är en påminnelse om att allmänna handlingar endast får gallras enligt de regler som återfinns i arkivlagen och meddelade gallringsbeslut.

En myndighet har skyldighet att arkivera allmänna handlingar oavsett handlingarnas informationsklassificering. Arkivet är en del av kulturarvet vilket alltid ska beaktas när

216 2 § Riksarkivets föreskrifter om gallring av handlingar rörande hanteringen av hemliga och kvalificerat hemliga handlingar hos myndigheter under Försvarsdepartementet.

handlingar gallras. Myndigheternas arkiv ska bevaras, hållas ordnade och vårdas så att de bl.a. tillgodoser rätten att ta del av allmänna handlingar.[217] I detta sammanhang kan även nämnas att Försvarsmakten i samråd med Krigsarkivet har fattat ett beslut när gallring får ske av handlingar av tillfällig eller ringa betydelse [referens 17].

Se även avsnitt 9.19.10 om undanförsel och förstöring i krig m.m.

> *Vid förstöring av en hemlig handling som utgörs av framställning i skrift eller bild och som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre får restprodukten utgöras av spån med en bredd av högst 1,2 mm och en längd av högst 15 mm eller av högst 2 x 2 mm kvadratiska spån.*
>
> *Vid förstöring av hemliga handlingar som avses i första stycket och som har placerats i informationssäkerhetsklassen HEMLIG/RESTRICTED får restprodukterna utgöras av spån med en bredd av högst 2,5 mm och en längd av högst 30 mm eller av högst 4 x 4 mm kvadratiska spån.*
>
> 2 kap. 16 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Dokumentförstörare som enbart uppfyller kraven för förstöring av handlingar som har placerats i informationssäkerhetsklass HEMLIG/RESTRICTED behöver tydligt märkas så att de inte används för förstöring av handlingar som är placerade i högre informationssäkerhetsklasser. En sådan märkning kan vara ”ENDAST FÖR HEMLIG/RESTRICTED”. Gamla och slitna destruktörer som inte till fullo uppfyller kraven för att användas för förstöring av hemliga handlingar i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL och högre kan oftast användas för förstöring av handlingar i informationssäkerhetsklassen HEMLIG/RESTRICTED.

Föreskriften innebär att förstöring i Försvarsmakten även får ske på ett sätt som ger restprodukter som inte utgörs av spån, t.ex. bränning där restprodukten utgörs av aska. I fråga om andra restprodukter än spån ska fortfarande 2 kap. 22 § Försvarsmaktens föreskrifter om säkerhetsskydd uppfyllas.

I de sällsynta fall en hemlig handling innehåller text eller annan information som är läsbar på ett spån (d.v.s. återskapande av uppgifterna är inte omöjliggjort) måste förstöringen ske på ett annat sätt, t.ex. bränning. En dokumentförstörare där restprodukten utgörs av spån som är mindre än vad som anges i 2 kap. 16 § Försvarsmaktens interna bestämmelse om säkerhetsskydd och skydd av viss materiel får användas.

217 3 § arkivlagen.

Förstöring av en hemlig handling som har placerats i informationssäkerhetsklassen HEMLIG/TOP SECRET ska skriftligen intygas av två, vid förstöringen samtidigt närvarande, försvarsmaktsanställda personer.

2 kap. 17 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Kravet på att förstöringen ska dokumenteras gäller även en sådan handling som inte är en allmän handling.

9.19.2 Utrikesklassificerade handlingar

Förstöring av utrikesklassificerade handlingar och materiel som innehåller utrikesklassificerade uppgifter ska i Försvarsmakten ske på samma sätt som för hemliga handlingar.[218]

9.19.3 Sekretessklassificerade handlingar

Vid förstöring av sekretessklassificerade handlingar som utgörs av framställning i skrift eller bild får restprodukterna utgöras av spån med en bredd av högst 2,5 mm och en längd av högst 30 mm eller av högst 4 x 4 mm kvadratiska spån.

3 kap. 8 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Krav i Försvarsmakten på restprodukter vid förstöring av sekretessklassificerade handlingar är detsamma som för hemliga handlingar som är placerade i informationssäkerhetsklass HEMLIG/RESTRICTED. Det finns ingen föreskrift om att förstöring av sekretessklassificerade handlingar ska ske på ett sådant sätt att åtkomst till och återskapande av uppgifterna ska vara omöjligt.

Sekretessklassificerade handlingar får även förstöras i en dokumentförstörare som är avsedd för förstöring av hemliga handlingar som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre.

Destruktionsanläggningar kan användas för förstöring av sekretessklassificerade handlingar. När sådana anläggningar används är det vanligt att det upphandlade företaget förser organisationsenheten med behållare för insamling av handlingar som ska förstöras. När sådana behållare transporteras från organisationsenheten till destruk-

218 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

tionsanläggningen behöver inte egen ansvarig personal följa med eller närvara under förstöringen. Det är av stor vikt att organisationsenheten säkerställer (t.ex. genom administrativa rutiner, utbildning och märkning) att hemliga handlingar inte förekommer i behållare som enbart är avsedda för sekretessklassificerade handlingar.

I de fall destruktionsanläggningar används för förstöring av hemliga handlingar får sekretessklassificerade handlingar blandas med hemliga handlingar som utfyllnad. I rutiner för förstöring av sekretessklassificerade handlingar bör beaktas vilka dokumentförstörare m.m. som finns vid organisationsenheten samt i vilken omfattning sekretessklassificerade handlingar förekommer.

För gallring av handlingar som är sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400) men som inte rör riket säkerhet gäller särskilda bestämmelser som meddelas av Riksarkivet.

3 kap. 9 § Försvarsmaktens föreskrifter om skydd för sekretess- och utrikesklassificerade uppgifter och handlingar

Föreskriften är en påminnelse om att allmänna handlingar endast får gallras enligt de regler som återfinns i arkivlagen och meddelade gallringsbeslut. Se kommentaren till 2 kap. 23 § Försvarsmaktens föreskrifter om säkerhetsskydd i avsnitt 9.19.1.

9.19.4 Metoder för förstöring av handlingar

De vanligaste metoderna för förstöring är mekanisk bearbetning och bränning.

Det finns ingen förteckning över godkända maskiner för förstöring. Istället finns krav som det är upp till respektive myndighet och organisationsenhet i Försvarsmakten att uppfylla (avsnitt 9.19.1-9.19.3). Det är nödvändigt att uppmärksamma kraven vid anskaffning av maskiner och tjänster för förstöring. Säkerhetskontoret vid MUST kan ge stöd för bedömning av olika förstöringsmetoder.

9.19.5 Dokumentförstörare

Dokumentförstörare är ofta av golvmodell med spånavskärare. Kapaciteten hos dokumentförstörare kan variera från enstaka ark upp till ca 20 ark beroende på maskinens prestanda och vikten på papperet.

Overheadfilm bör inte destrueras i en dokumentförstörare, då den kan fastna i skärverket. Vissa dokumentförstörare kan ta en overheadfilm i taget om man lägger vanliga pappersark på bägge sidor. *Gem* får inte föras in i dokumentförstörare och man bör även undvika *häftklammer*, då dessa sliter på spånavskärarna.

Om *kryptonycklar* med streckkod ska förstöras i en dokumentförstörare som ger avlånga spån, av högst 15 mm längd och högst 1,2 mm bredd, gäller att kryptonyckeln ska matas in i dokumentförstöraren med långsidan före så att inte restprodukterna består av flera läsbara streckkoder.

Destruktörernas knivar måste *smörjas* för att fungera på ett tillfredsställande sätt. Den bästa smörjeffekten uppnås genom att man oljar in ett papper med lämplig olja, täcker detta papper med ytterligare ett papper samt matar in dessa två papper tillsammans i dokumentförstöraren. Alternativt häller man olja på ett läskpapper, låter papperet suga upp oljan under några sekunder och därefter matar in papperet i dokumentförstöraren.

9.19.6 Centraldestruktörer

Centraldestruktörer är större maskiner som ofta har roterande knivar och utbytbara raster.

Rasterhål med en diameter på högst 10 mm ger godtagbar storlek på restprodukterna. Använder man sig dessutom av ventilerad utsugning av restprodukterna får man ännu större säkerhet. Kapaciteten vid förstöring varierar mellan ca 40-200 kg/tim. För att öka säkerheten kan de hemliga handlingarna blandas med handlingar som inte är placerade i informationssäkerhetsklass.

9.19.7 Specialdestruktörer

Speciella destruktörer finns för förstöring av skrivmaskinsband, bandkassetter, disketter och liknande material. Vissa av dessa kan även användas för förstöring av pappershandlingar.

9.19.8 Destruktionsanläggningar

I Sverige finns destruktionsanläggningar som genom mekanisk bearbetning eller bränning förstör hemliga handlingar och materiel som innehåller hemliga uppgifter. Några är kontrollerade av Försvarsmakten och Rikspolisstyrelsen.

Egen ansvarig personal måste alltid vara med under hela förstöringen. Personalen vid anläggningen ska inte ha möjlighet att ta del av de handlingar och materiel som ska förstöras. Kontroll av restprodukterna måste utföras för att säkerställa att allt material är fullständigt förstört. Vid bränning behöver okulär kontroll av att förbränningsugnen verkligen är i drift genomföras.

Om transportband används vid en destruktionsanläggning är det av stor vikt att kontrollera att inga handlingar eller materiel har fallit vid sidan av transportbandet samt att restprodukten håller måttet för att vara fullständigt förstört. Destruktionsanlägg-

ningar kan ha som krav att handlingarna och materielen som ska förstöras ska vara packade i lådor. Att handlingarna och materielen är packade i lådor underlättar även övervakning under förstöring.

9.19.9 Bränning

Förstöring genom bränning är en effektiv förstöringsmetod om den sker så att bränningen underhålls med luft. I de fall förstöring inte kan ske lokalt i en dokumentförstörare (tuggning) eller genom bränning i en destruktionsanläggning kan bränning genomföras i tunna eller kar utomhus. Svårigheterna att uppnå en fullständig förbränning ska inte underskattas. Det är viktigt att se till att fullständig bränning sker så att uppgifter inte är avläsbara på t.ex. papper. Det är lämpligt att använda verktyg för att röra om i elden och ytterligare material för att underhålla den.

Bränning i destruktionsanläggning (avsnitt 9.19.8) är effektivt för stora mängder papper och materiel som ska förstöras. Det är också en lämplig metod att förstöra plastbaserade informationsbärare (t.ex. CD-skivor, videoband, fotografier etc.). Förstöring av lagringsmedier beskrivs i avsnitten 12.2.16 och 12.2.17.

9.19.10 Undanförsel och förstöring i krig m.m.

Informationstillgångar kan om de faller i orätta händer orsaka skada för Sverige. I lagen om undanförsel och förstöring finns föreskrifter som främst ska tillämpas då Sverige är i krig. Föreskrifterna omfattar även manuella eller IT-baserade informationstillgångar.[219] Föreskrifterna i lagen tar över arkivlagens föreskrifter om vilka handlingar som får gallras.[220] Om planläggning för undanförsel och förstöring genomförs är det nödvändigt att den även omfattar informationstillgångar hos myndigheter och enskilda (t.ex. företag).

I stridssituationer, t.ex. då Försvarsmakten deltar i en internationell militär insats eller nationellt försvar, kan situationer förekomma där en militär chef även på förhållandevis låg nivå av taktiska skäl måste besluta att informationstillgångar som ska bevaras ska förstöras. Någon föreskrift som medger en sådan förstöring finns idag inte. Ett sådant handlande får bedömas i efterhand med utgångspunkt i de allmänna reglerna om nöd i brottsbalken.[221] [222] Det är av större vikt att uppgifter som kan hjälpa en motståndare inte röjs till denne.

219 Sidan 1, Undanförsel och förstöring prop. 1992/93:78.
220 10 § tredje stycket arkivlagen.
221 Sidan 6, Undanförsel och förstöring prop. 1992/93:78.
222 24 kap. 4 § brottsbalken.

Hotet att informationstillgångar röjs till obehöriga genom intrång i förvaringsutrymmen till följd av strider, uppror, plundring etc. bör uppmärksammas i säkerhetsanalys för verksamheten.

Förstöring av informationstillgångar bör prioriteras utifrån den skada som uppstår vid ett röjande. Informationstillgångar som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET bör därför förstöras först tillsammans med kryptonycklar som inte längre behövs. I verksamheter där register över allmänna handlingar innehåller hemliga uppgifter är det viktigt att även sådana register förstörs (avsnitt 9.8.3).

9.20 Intern distribution

9.20.1 Hemliga handlingar

Föreskrifter om hur *intern distribution* av hemliga handlingar ska utföras inom en myndighet saknas i Försvarsmaktens föreskrifter om säkerhetsskydd. För en organisationsenhet i Försvarsmakten finns det heller inte några sådana föreskrifter i interna bestämmelser. Stöd för hur sådan intern distribution ska ordnas får sökas i övriga föreskrifter.

Normalt distribueras hemliga handlingar inom en myndighet via en expedition eller motsvarande. Det kan finnas behov av att inom en myndighet även distribuera hemliga handlingar som inte är allmänna handlingar (hemliga arbetshandlingar). Även intern distribution av hemliga handlingar som är allmänna handlingar och som inte är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre, och därför inte omfattas av krav på exemplarhantering, kan distribueras internt på ett annat sätt än via en expedition.

En vanlig ordning vid intern distribution av en hemlig handling är att en anställd som ska hämta en hemlig handling får en avisering om detta via e-post eller som pappersslapp i den anställdes postfack.

Grundläggande för intern distribution av alla former av hemliga handlingar är att den måste utformas så att obehöriga inte kan komma åt en hemlig handling. Centralt är hur en hemlig handling *förvaras* under distributionen (avsnitt 9.11). Föreskrifterna om förvaring av hemliga handlingar gäller även då handlingarna ska förvaras under intern distribution (exempel 9:16 och exempel 9:17).

Exempel 9:16

Inom förbandets stab används öppna postfack för distribution av hemliga handlingar. Postfacken är placerade i en korridor där personal i staben, lokalvårdare och besökare kan uppehålla sig. En person som inte är behörig till de hemliga handlingarna och som uppehåller sig i korridoren kan komma åt handlingarna och ta del av uppgifterna i handlingarna. Förvaringen av de hemliga handlingarna i de öppna postfacken uppfyller inte föreskrifterna i 2 kap. 13-17 §§ Försvarsmaktens föreskrifter om säkerhetsskydd. Den interna distributionen är ur säkerhetssynpunkt otillräcklig.

Exempel 9:17

Vid en myndighet används låsbara postfack i tunnplåt (skyddsnivå 1) för distribution av hemliga handlingar som är placerade i informationssäkerhetsklass HEMLIG/RESTRICTED. Postfacken är placerade vid myndighetens expedition och varje anställd har ett eget postfack och de kan endast öppna sitt eget postfack.

Distribution av hemliga handlingar som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre sker via expeditionen där de förvaras i ett valv. Förvaringen i de låsbara postfacken och valvet uppfyller föreskrifterna i 2 kap. 13-15 §§ samt 3 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Den interna distributionen är ur säkerhetssynpunkt tillräcklig i fråga om förvaringen.

Om distribution av hemliga handlingar som är placerade i informationssäkerhetsklass HEMLIG/RESTRICTED sker i låsbara postfack i tunnplåt (exempel 9:17) får postfacket även användas för distribution av handlingar som inte innehåller uppgifter som omfattas av sekretess. Det kan i sådana fall vara lämpligt att de hemliga handlingarna läggs i röda plastmappar eller liknande för att undvika sammanblandning med övriga handlingar.

Hemliga handlingar får inte distribueras internt genom distribution som endast är avsedda för handlingar som inte är hemliga, sådan distribution kan benämnas öppen postdistribution. Här kan nämnas att en hemlig handling som läggs i ett ytterkuvert, för att dölja att det är fråga om en hemlig handling, inte är en tillräcklig skyddsåtgärd för att kunna distribuera den hemliga handlingen.

I intern distribution av hemliga handlingar som sker via en expedition kan ett kuvert användas för hemliga handlingar för att dölja innehållet om kuvertet märks med informationssäkerhetsklass och mottagarens namn.

9.20.2 Utrikesklassificerade handlingar

Föreskrifter om hur *intern distribution* av utrikesklassificerade handlingar ska utföras saknas i Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Avsnitt 9.20.1 om intern distribution av hemliga handlingar gäller i Försvarsmakten även för intern distribution av utrikesklassificerade handlingar.[223]

9.20.3 Sekretessklassificerade handlingar

Det finns inga krav på skydd vid distribution av en sekretessklassificerad handling.[224] Det finns således inga krav på skydd för att en sådan handling inte röjs under distribution. Sedvanlig intern distribution av försändelser (s.k. öppen post) och handlingar internt inom organisationsenhet är tillräcklig.

Öppna budkuvert bör inte användas för intern distribution av en sekretessklassificerad handling. Det är lämpligt att använda ett förslutet kuvert för intern distribution av en sådan handling. Av kuvertet bör det förutom mottagarens namn eller befattning då framgå att det innehåller en sekretessklassificerad handling.

9.21 Extern distribution

Distribution av handlingar behöver inte endast ske genom en fysisk förflyttning. Hemliga handlingar kan ofta även distribueras genom ett godkänt krypterat sambandsmedel (t.ex. krypterad telefax) eller genom funktioner i ett IT-system (t.ex. e-post). Om möjligt bör funktioner i IT-system användas för distribution av handlingar som redan är lagrade i elektronisk form då detta bevarar informationsinnehållet och medger vidare förädling av handlingens innehåll.

Obehöriga har större möjligheter att ta del av uppgifter i en handling som fysiskt, eller representerad i elektronisk form (t.ex. ett USB-minne), överförs utanför en myndighets lokaler och områden. Sådana handlingar behöver därför skyddas så att obehöriga inte kan ta del av uppgifterna och om möjligt upptäcka om så har skett. Skyddet för distribution av handlingar skiljer sig åt för handlingar som hör till olika sekretesskategorier.

223 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

224 Föreskrift om distribution saknas i 3 kap. Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

9.21.1 Hemliga handlingar

Varje myndighet skall besluta hur försändelser med hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre skall sändas från och tas emot av myndigheten. Myndigheten skall se till att erforderliga skyddsåtgärder vidtas under distributionen.

En försändelse med hemliga handlingar som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre skall sändas med en distributör som har godkänts av myndigheten.

2 kap. 24 § Försvarsmaktens föreskrifter om säkerhetsskydd

Hemliga handlingar som inte distribueras med sambandsmedel som på ett godkänt sätt krypterar uppgifterna i handlingen, får endast försändas i förseglat emballage enligt särskilda rutiner som respektive myndighet utarbetar. Även hemliga handlingar som är placerade i informationssäkerhetsklass HEMLIG/RESTRICTED bör distribueras på motsvarande sätt som de handlingar som har placerats i högre informationssäkerhetsklass eftersom andra rutiner inte garanterar att försändelsen når mottagaren med tillräcklig säkerhet.

En rutin för distribution bör innehålla åtgärder för att upptäcka om ett emballage under distributionen har öppnats och ersatts med ett nytt emballage.

För att ge de distribuerade handlingarna ett högre skydd än vad ett enbart förseglat emballage ger, t.ex. om distributören skulle bli utsatt för rånförsök, bli sjuk, skadas vid en trafikolycka, bör man använda ett distributionsutrymme som, i händelse av intrångsförsök i detsamma, fysiskt förstör handlingarna. Ett annat alternativ är att ge de transporterade handlingarna ett fysiskt skydd, t.ex. i form av ett litet säkerhetsskåp (enligt SS 3492) eller motsvarande förvaringsutrymme som är monterat i transportfordonet.

En brännväska är ett exempel på ett distributionsutrymme som fysiskt förstör handlingarna. Om någon manipulerar väskans lås eller på annat sätt försöker bryta sig in i den utlöses brännpatroner som förstör väskans innehåll och därmed avsevärt försvårar åtkomst av de hemliga uppgifterna. Väskan kan anordnas för transport, och då även förstöring, för olika sorters medier såsom papper, film och mjuka magnetiska lagringsmedier. Innan en brännväska används måste man bestämma sig för vilket medium (papper, film, mjuka magnetiska lagringsmedier) som ska distribueras och anordna väskan och dess brännfunktion efter detta. En sådan brännväska är inte lämplig för distribution av hårddiskar och elektroniska minnen (t.ex. USB-minnen).

Om en myndighet före den 1 januari 2004 har beslutat hur försändelser med hemliga respektive kvalificerat hemliga handlingar ska sändas från och tas emot av myndigheten, gäller detta beslut.[225]

> *Hemliga handlingar som inte distribueras med sambandsmedel som krypterar uppgifterna i handlingen får endast försändas i förseglat emballage. Emballaget ska vara så beskaffat att det är omöjligt att ta del av uppgifterna i handlingen utan att bryta emballaget. Förseglingen ska vara sådan att det går att se om någon har brutit emballaget.*
>
> *Om mängden hemliga handlingar medför att distribution enligt första stycket inte kan eller bör ske ska bestämmelserna i 21, 22, 24-28 och 30-35 §§ i detta kapitel tillämpas.*
>
> 2 kap. 18 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Ett förseglat emballage bör bestå av säkerhetskuvert (avsnitt 9.21.2), sådana kuvert beställs via Försvarets bok- och blankettförråd i Arboga.

Andra stycket avser föreskrifter i Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel om transport av hemliga handlingar.

> *Den som av en distributör tar emot en försändelse som avses i 18 § i detta kapitel ska kontrollera att försändelsen överensstämmer med följesedeln (motsv.) och att förseglingen och försändelsen i övrigt är oskadad. Är försändelsen skadad ska den som tar emot försändelsen se till att distributören gör anteckning om skadans beskaffenhet. Vidare ska den som tar emot försändelsen anmäla skadan till avsändaren.*
>
> 2 kap. 19 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

225 Ikraftträdande- och övergångsbestämmelse 6 d i Försvarsmaktens föreskrifter om säkerhetsskydd.

Den som slutligen tar emot en försändelse ska kontrollera att förseglingen och försändelsen i övrigt är oskadad och att innehållet överensstämmer med uppgifterna i huvudhandlingen, missivet eller sändlistan. Om försändelsen är skadad eller uppgifterna inte stämmer överens ska avsändaren underrättas.

Finns ingen anledning till anmärkning ska eventuella sigill förstöras så att de inte går att återanvända.

2 kap. 20 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

Om en försändelse är skadad ska skadan även rapporteras till organisationsenhetens säkerhetsorganisation. En sådan rapport ska vidarebefordras till MUST.[226]

9.21.2 Säkerhetskuvert

Säkerhetskuvert används i Försvarsmakten och andra statliga myndigheter för distribution av handlingar. Säkerhetskuverten är engångsförpackningar av plast som efter att de har förslutits inte obemärkt ska kunna öppnas. Säkerhetskuverten hindrar inte en person från att öppna kuvertet, den eftersökta egenskapen är att detektera ett intrång i ett säkerhetskuvert.

Bild 9:22 visar hur förslutningen på ett säkerhetsemballage ser ut när förslutningen inte påverkats. Bild 9:23 visar hur förslutningen ser ut efter försök att öppna säkerhetsemballaget.

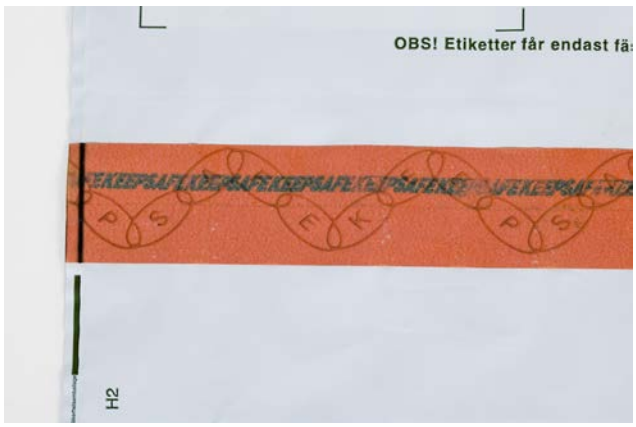


Bild 9:22 - Säkerhetsemballage där förslutningen inte har påverkats.

226 1 kap. 6 § andra stycket Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

Bild 9:23 - Säkerhetsemballage där ett mönster framträder på emballaget och på förslutningen efter försök att öppna förslutningen.

Säkerhetskuvert har en begränsad livslängd. Bäst före datum infaller två år efter tillverkning. Ett säkerhetskuvert får inte användas i Försvarsmakten efter att dess bäst före datum har infallit.

För användning av Säkerhetskuvert M7102-122740 (Värde) samt Säkerhetskuvert (Rek) M7102-122730 gäller i Försvarsmakten att en person som ska använda ett sådant kuvert ska genomföra en visuell kontroll avseende kuvertbottens skick. Vidare ska kuvertbotten kontrolleras genom att personen med handkraft trycker på kuvertbotten inifrån och därvid konstatera att kuvertet inte är defekt. Vid konstaterad felaktighet på kuvert ska detta skyndsamt anmälas till lokal expedition samt organisationsenhetens säkerhetschef [referens 33].

9.21.3 Utrikesklassificerade handlingar

Distribution av utrikesklassificerade handlingar och materiel som innehåller utrikesklassificerade uppgifter ska i Försvarsmakten ske på samma sätt som för hemliga handlingar.[227]

9.21.4 Sekretessklassificerade handlingar

Det finns inga krav på skydd vid distribution av en sekretessklassificerad handling.[228] Det finns således inga krav på skydd för att en sådan handling inte röjs under distribution. Sedvanlig distribution av försändelser (genom Posten eller motsvarande distributör) är tillräcklig.

227 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

228 Föreskrift om distribution saknas i 3 kap. Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Det är lämpligt att använda ett förslutet kuvert för extern distribution av en sekretessklassificerad handling. Av kuvertet bör det då inte framgå att det innehåller en sekretessklassificerad handling.

Se avsnitt 10.3 om kryptering vid överföring av sekretessklassificerade uppgifter.

9.22 Distribution utomlands

Avsnitt 9.21 om extern distribution gäller även för handlingar som ska distribueras till utlandet.

9.22.1 Hemliga handlingar

> ***För försändelser med hemliga handlingar till utlandet skall Utrikesdepartementets kurirförbindelser anlitas.***
>
> ***Rikspolisstyrelsen och Försvarsmakten kan för sina respektive tillsynsområden enligt 39 § besluta om undantag från första stycket.***
>
> 11 § säkerhetsskyddsförordningen

Skyddet för handlingar som skickas utomlands är lägre än i Sverige varför Utrikesdepartementets kurirförbindelser normalt ska användas för distribution av hemliga handlingar, t.ex. mellan en svensk myndighet och en försvarsavdelning vid en av Sveriges ambassader.

> *I 11 § första stycket säkerhetsskyddsförordningen (1996:633) finns föreskrifter om försändelser med hemliga handlingar till utlandet.*
>
> *Hemliga handlingar som sänds utomlands skall förses med anteckning om uppgifternas ursprungsland.*
>
> *Varje myndighet får i avtal med ett annat land eller mellanfolklig organisation komma överens om att distribuera hemliga handlingar på annat sätt än vad som föreskrivs i 11 § första stycket säkerhetsskyddsförordningen (1996:633).*
>
> 2 kap. 25 § Försvarsmaktens föreskrifter om säkerhetsskydd

För distribution av hemliga handlingar till en svensk kontingent i utlandet kan inte alltid Utrikesdepartementets kurirförbindelser användas. Distributionen kan i sådana fall arrangeras som en transport av hemliga handlingar. Distributionen underlättas då transporten genomförs av Försvarsmaktens personal i militärt fartyg, luftfartyg eller fordon.

I avsnitt 9.3 beskrivs märkning om uppgifternas ursprungsland.

I internationella samarbeten med andra stater och mellanfolkliga organisationer, och där hemliga handlingar ska utbytas mellan Försvarsmakten och den andra staten eller mellanfolkliga organisationen, kan distributionen av handlingarna behöva ske på ett annat sätt än genom Utrikesdepartementets kurirförbindelser. Hur distributionen i sådana fall ska genomföras ska då överenskommas med den andra staten eller mellanfolkliga organisationen.

Att det finns regelverk för hur hemliga handlingar ska distribueras för att överlämnas till en annan stat eller mellanfolklig organisation innebär inte att alla uppgifter som omfattas av sekretess enligt OSL får lämnas över. I avsnitt 7.7 beskrivs behörighet för utländsk personal.

9.22.2 Utrikesklassificerade handlingar

> *För försändelser med utrikesklassificerade handlingar till och från utlandet ska Utrikesdepartementets kurirförbindelser om möjligt anlitas.*
>
> 2 kap. 5 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Den normala principen för att sända handlingar som innehåller utrikesklassificerade uppgifter utomlands är att använda Utrikesdepartementets kurirförbindelser. Detta framgår av flera bilaterala säkerhetsskyddsavtal som Sverige har ingått med många länder. Syftet med att använda denna rutin är att handlingarna ges ett skydd mot obehörig åtkomst genom att kuriren ständigt har full uppsikt över försändelsen under transporten. I vissa fall finns det undantag från denna hanteringsrutin.

I vissa bilaterala säkerhetsskyddsavtal finns det möjligheter för de nationella säkerhetsmyndigheterna att komma överens om andra rutiner om detta anses vara mer ändamålsenligt i det specifika fallet. Det kan t.ex. röra sig om transporter mellan Sverige och ett annat land av information som rör ett specifikt försvarsmaterielprojekt och där transportvägen mellan länderna anses säker även utan det skydd som kurirverksamheten ger.

9.22.3 Sekretessklassificerade handlingar

Det finns inga krav på skydd vid distribution av en sekretessklassificerad handling utomlands.[229] Det finns således inga krav på skydd för att en sådan handling inte röjs

229 Föreskrift om distribution saknas i 3 kap. Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

när den distribueras utomlands. Sedvanlig distribution av försändelser (t.ex. genom Posten eller motsvarande distributör utomlands) är tillräcklig.

I de fall krav på distribution av sekretessklassificerade handlingar har avtalats inom ramen för ett visst internationellt samarbete gäller sådana krav.[230]

230 3 kap. 20 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

10 Skydd mot obehörig avlyssning i ett elektroniskt kommunikationsnät

Med ett *elektroniskt kommunikationsnät* avses i detta avsnitt *system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.*[231] Begreppet *elektroniskt kommunikationsnät* är lämpligt att använda i fråga om skydd mot obehörig avlyssning då begreppet avses vara heltäckande och omfattar t.ex. såväl telefoni, bildöverföring, kommunikation i ett IT-system som mellan IT-system.

10.1 Hemliga uppgifter

Myndigheter och andra som förordningen gäller för skall, innan de sänder hemliga uppgifter i ett datanät utanför deras kontroll, förvissa sig om att det för uppgifterna där finns en fullgod informationssäkerhet.

Hemliga uppgifter får krypteras endast med kryptosystem som har godkänts av Försvarsmakten.

13 § säkerhetsskyddsförordningen

Säkerhetsskyddet ska förhindra att hemliga uppgifter obehörigen röjs, ändras eller förstörs, vare sig detta sker uppsåtligen eller av oaktsamhet.[232] När sådana uppgifter sänds i ett elektroniskt kommunikationsnät måste det därför finnas ett skydd för uppgifterna så att de t.ex. inte kan avlyssnas. Godkänd kryptering är en skyddsåtgärd för uppgifter som sänds i ett elektroniskt kommunikationsnät som inte står under en myndighets kontroll.

Föreskriften innebär inte att hemliga uppgifter helt utan säkerhetsskydd får sändas i ett elektroniskt kommunikationsnät som står under en myndighets kontroll (t.ex. en interntelefonanläggning i en byggnad som disponeras av en myndighet). Skyddsåtgärder för ett sådant nät ska vidtas utifrån myndighetens säkerhetsanalyser avseende vilka hot, risker och sårbarheter som kan påverka en myndighets verksamhet som är av betydelse för rikets säkerhet.[233] Skyddet för ett sådant nät får bestå av andra skydds-

231 1 kap. 7 § lagen om elektronisk kommunikation.
232 Sidorna 26-27, Säkerhetsskydd prop. 1995/96:129.
233 1 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd.

åtgärder än kryptering. För ett elektroniskt kommunikationsnät som står under en myndighets kontroll kan kryptering dock vara den lämpligaste skyddsåtgärden.
I IT-system kan det finnas inbyggda kryptografiska metoder för skydd av de behandlade uppgifterna. Om en sådan kryptografisk metod inte har godkänts av Försvarsmakten ger funktionen inte något säkerhetsskydd.

Ett godkännande enligt andra stycket beslutas i Försvarsmakten av chefen för MUST eller den han eller hon bestämmer.[234]

Då föreskriften inte gäller alla myndigheter kan det således förekomma att hemliga uppgifter inte ges en fullgod informationssäkerhet då de sänds i ett elektroniskt kommunikationsnät som inte står under en sådan myndighets kontroll. Av samma anledning kan hemliga uppgifter komma att sändas utan att de först har krypterats eller komma att krypteras med ett kryptosystem som inte har godkänts av Försvarsmakten.[235] [236]

Att skydda hemliga uppgifter med ett *utländskt kryptosystem* är att likställa med att delge uppgifterna till den stat eller mellanfolkliga organisation som har tillgång till de kryptonycklar som används för att kryptera uppgifterna. Se H SÄK Grunder om avtal i internationell verksamhet.

För signalskyddstjänsten gäller särskilda bestämmelser i fråga om hantering av kryptonycklar och signalskyddsmateriel samt användning av kryptografiska funktioner.

1 kap. 9 § Försvarsmaktens föreskrifter om säkerhetsskydd

Signalskyddstjänst syftar till att, med hjälp av kryptografiska metoder och övriga signalskyddsåtgärder, förhindra obehörig insyn i och påverkan av telekommunikations- och IT-system.[237] Med särskilda bestämmelser avses Försvarsmaktens föreskrifter om signalskyddstjänsten inom totalförsvaret som gäller för statliga myndigheter. För ytterligare information om signalskydd se H TST Grunder.

234 9 § Försvarsmaktens interna bestämmelser om signalskyddstjänsten.
235 1-2 §§ säkerhetsskyddsförordningen.
236 33 § förordning med instruktion för Försvarsmakten.
237 H SÄK Grunder.

10.2 Utrikesklassificerade uppgifter

Utrikesklassificerade uppgifter som förmedlas i ett elektroniskt kommunikationsnät utanför Försvarsmaktens kontroll ska krypteras med kryptosystem som har godkänts av chefen för militära underrättelse- och säkerhetstjänsten i Högkvarteret eller den han eller hon bestämmer.

1 kap. 14 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Föreskriften motsvaras av 13 § säkerhetsskyddsförordningen. Föreskriften gäller endast Försvarsmakten. För andra myndigheter finns inget krav på kryptering av utrikesklassificerade uppgifter. Försvarsmakten rekommenderar att andra myndigheter krypterar utrikesklassificerade uppgifter enligt vad som gäller för hemliga uppgifter.

För signalskyddstjänsten gäller särskilda bestämmelser i fråga om hantering av kryptonycklar och signalskyddsmateriel samt användning av kryptografiska funktioner.

1 kap. 13 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Med särskilda bestämmelser avses Försvarsmaktens föreskrifter om signalskyddstjänsten inom totalförsvaret och Försvarsmaktens interna bestämmelser om signalskyddstjänsten.

10.3 Sekretessklassificerade uppgifter

Det finns normalt inget författningskrav på att sekretessklassificerade uppgifter ska krypteras innan uppgifterna sänds i ett elektroniskt kommunikationsnät. Vid överföring av sekretessklassificerade uppgifter via Internet rekommenderas där så är möjligt kryptering med *krypto för skyddsvärda uppgifter* (KSU). KSU är avsett för skydd av information som är sekretessbelagd enligt OSL och annan information som en organisationsenhet väljer att skydda. KSU får dock inte användas för skydd av hemliga eller utrikesklassificerade uppgifter (se I KSU).

I Försvarsmakten har juridiska staben beslutat att känsliga personuppgifter ska krypteras när de kommuniceras utanför FM IP-nät över ett öppet nätverk [referens 15]. Med öppet nätverk avses enligt beslutet sådana nätverk som går utanför FM IP-nät och lämnar Försvarsmakten. I Försvarsmakten finns även andra elektroniska kommunikationsnät. Det är därför lämpligt att använda kryptering då känsliga personupp-

gifter kommuniceras utanför något sådant nätverk och lämnar Försvarsmakten. Som exempel på kommunikation över ett öppet nätverk kan nämnas att en anställd skickar känsliga personuppgifter till sin privata e-postadress via Internet eller för över uppgifterna på ett USB-minne och sedan kopplar in detta på en annan dator än inom FM IP-nät. Sådana uppgifter kan krypteras med krypto för skyddsvärda uppgifter (KSU) (se I KSU).

10.4 Användning av svenska signalskyddssystem för att skydda Nato- och EU-uppgifter

För vad som gäller vid användning av svenska signalskyddssystem för att skydda Nato- och EU-uppgifter hänvisas till [referens 31] respektive [referens 20].

10.5 Kryptering i andra fall

I de fall avlyssningshotet är stort och informationsförluster bedöms påverka verksamheten negativt är kryptering en lämplig skyddsåtgärd även för uppgifter som är sekretessklassificerade eller uppgifter som inte omfattas av sekretess enligt OSL. Det kan t.ex. vara fråga om telefoni och Internet som går via satellitförbindelser och som används såväl i tjänsten som privat (s.k. welfare) av Försvarsmaktens personal i en internationell militär insats.

12 Lagringsmedier

Ett lagringsmedium är ett *permanent minnesmedium som används för att kunna lagra och läsa uppgifter*.[248] Även om definitionen står i en författning som rör säkerhetsskydd används begreppet lagringsmedium i Försvarsmakten även för andra lagringsmedier som inte avses innehålla och som inte innehåller hemliga uppgifter. Exempel på ett lagringsmedium är hårddiskar med roterande magnetiska skivor, SSD-diskar, CD-ROM, DVD, Blu-ray, disketter, ZIP-diskar, backupband, USB-minnen och aktiva kort.

De beskrivna föreskrifterna om lagringsmedier avser minnesmedier som vid avsaknad av ström behåller data som är lagrad. Ett minnesmedium där all data raderas när strömmen bryts (s.k. *icke-permanent minnesmedium*, flyktigt minne eller volatile memory på engelska) omfattas inte av föreskrifterna om lagringsmedier. Om ett sådant icke-permanent minnesmedium innehåller en hemlig uppgift utgör det *hemlig materiel* och ska ges ett säkerhetsskydd. Ett exempel på ett icke-permanent minnesmedium är RAM-minne (Read Access Memory) i en dator.

I arkivsammanhang används begreppet *databärare* istället för lagringsmedium.[249]

Med *fast monterat lagringsmedium* avses i denna handbok ett lagringsmedium som är monterat i en utrustning. Normalt kan ett sådant lagringsmedium inte avlägsnas ur utrustningen utan att utrustningen öppnas och lagringsmediet monteras ur. Några exempel på fast monterade lagringsmedier är:

- En arbetsplatsdator som du skruvar isär och tar ut hårddisken ur.
- Nätverksutrustning (t.ex. en router) som innehåller ett fast monterat lagringsmedium.
- Hårddiskar som ingår i en lagringslösning som består av rackmonterade hårddiskar.
- Ett elektroniskt minne som är inbyggt i en mobiltelefon.

Med *flyttbart lagringsmedium* avses i denna handbok ett lagringsmedium som inte är fast monterat.

I Försvarsmakten förekommer även andra utryck som då avser en kategori av lagringsmedier. Ett exempel är *mobil extern lagringsenhet* som enligt auktorisationsbeslut [referens 43] använder USB eller Firewire och som är avsett för sekretessklassifi-

248 7 kap. 1 § 1 Försvarsmaktens föreskrifter om säkerhetsskydd.
249 2 kap. 1 § Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling).

cerade uppgifter. Auktorisationsbeslutet innehåller krav på egenskaper som gäller för mobila externa lagringsenheter och IT-system där sådana flyttbara lagringsmedier ska användas.

12.1 Flyttbara lagringsmedier

Att flytta information mellan flera IT-system med hjälp av ett flyttbart lagringsmedium är idag enkelt och går mycket snabbt. Ett *USB-minne* är ett exempel på ett av de idag vanligaste flyttbara lagringsmedierna.

Flyttbara lagringsmedier innebär många fördelar, men medför även risker. Ofta lagras mycket mer information på ett USB-minne än vad innehavaren egentligen behöver ha med sig. När minnet sedan tappas bort eller stjäls förloras en mycket stor mängd uppgifter vilket kan medföra onödiga konsekvenser. Ett USB-minne bör endast användas för tillfällig lagring av uppgifter. Uppgifter som inte längre behövs för arbetet bör tas bort, även om uppgifterna skulle kunna återskapas.

I samarbeten med andra myndigheter, företag, andra stater och mellanfolkliga organisationer kan det finnas ett behov att i Försvarsmaktens IT-system använda ett lagringsmedium som inte har sitt ursprung i Försvarsmakten. Ett exempel är när en utomstående besöker Försvarsmakten för att föreläsa och lagrar sin presentation på ett medfört USB-minne. Verksamhetens behov att kunna ansluta sådana lagringsmedier behöver uppmärksammas i säkerhetsmålsättningen för det IT-system som är tänkt att användas.

Före användning av ett flyttbart lagringsmedium är det därför viktigt att kontrollera vilka bestämmelser som gäller för det IT-system som det ska användas i, och vem lagringsmediet tillhör. Om det inte står klart vilka bestämmelser som gäller måste organisationsenhetens IT-säkerhetschef eller säkerhetschef kontaktas.

Flyttbara lagringsmedier kan även användas för att sprida skadlig kod. En metod att föra in skadlig kod i IT-system är att plantera i förväg preparerade USB-minnen, t.ex. på en parkeringsplats eller i anslutning till arbetsplatsen. Ett upphittat eller på annat sätt okänt lagringsmedium ska därför aldrig anslutas till Försvarsmaktens IT-system. Sådana okända lagringsmedier ska alltid överlämnas till den lokala säkerhetsorganisationen.

Försvarsmakten tillhandhåller USB-minnen till alla anställda som behöver ett (avsnitt 12.3). Det är sådana USB-minnen som anställda ska använda i Försvarsmaktens IT-system. I Försvarsmakten får inte de anställdas privata lagringsmedier användas i Försvarsmaktens IT-system, eftersom systemen inte är auktoriserade och ackrediterade för sådan användning.

12.2 Säkerhetsskydd för lagringsmedier

Ett lagringsmedium som avses innehålla eller som innehåller hemliga uppgifter skall ha ett säkerhetsskydd som motsvarar det säkerhetsskydd som gäller för den informationssäkerhetsklass som lagringsmediet har placerats i.

7 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd

Föreskriften är en portalparagraf för säkerhetsskydd avseende lagringsmedier och innebär att föreskrifterna i 2 kap. Försvarsmaktens föreskrifter om säkerhetsskydd ska tillämpas av en myndighet även i fråga om lagringsmedier. I Försvarsmakten gäller dessutom att 2 kap. Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel även ska tillämpas på lagringsmedier. Vissa av föreskrifterna blir dock endast tillämpbara i fråga om pappersdokument. T.ex. kravet i 2 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd om att varje sida i en hemlig handling som består av flera sidor ska innehålla en hänvisning till uppgiften om informationssäkerhetsklass på första sidan. Bild 12:2 visar en handlings livscykel och skyddsåtgärder under livscykeln, dessa gäller i Försvarsmakten även för lagringsmedier som avses innehålla eller som innehåller hemliga uppgifter.

7 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd anger att de lagrade uppgifternas betydelse, d.v.s. placering i informationssäkerhetsklass, ska styra ett lagringsmediums säkerhetsskydd oavsett om det innehåller eller anses utgöra en allmän handling. Statusen enligt TF saknar betydelse för vilket säkerhetsskydd som ett lagringsmedium ska ha. Följande fyra punkter visar varför det inte är adekvat att använda begreppet allmän handling för att avgöra vilket säkerhetsskydd som ett lagringsmedium ska ha.

1. Lagringsmedier används för lagring av uppgifter som ingår i allmänna handlingar och i handlingar som inte är allmänna (s.k. arbetshandlingar). I fråga om handlingar som skapas i IT-system kan statusen på sådana handlingar och kopior av dessa skifta, t.ex. i samband med att en sådan lagrad handling har expedierats.[250]

2. I TF används begreppet *upptagning för automatiserad behandling* och avser då bl.a. uppgifter som lagras på ett lagringsmedium. En upptagning är en handling.[251] I fråga om en databas eller ett register kan varje konstellation av sakligt sammanhängande uppgifter ses som en upptagning för sig.[252] Det kan därför vara svårt att på förhand avgöra vilka s.k. *potentiella handlingar*[253] som ett

250 Sidorna 36-39 och 41-42, Allmänna handlingar i elektronisk form – offentlighet och integritet (SOU 2010:4).
251 2 kap. 3 § TF.
252 Sidan 90, Om nya grundlagsbestämmelser angående allmänna handlingars offentlighet prop.1975/76:160.
253 Sidan 34, Allmänna handlingar i elektronisk form – offentlighet och integritet (SOU 2010:4).

lagringsmedium innehåller. Uppgifter i *färdiga elektroniska handlingar* (slutligt utformade handlingar i elektronisk form med ett bestämt, fixerat innehåll, t.ex. e-post) bildar inte potentiella handlingar.[254] Ett lagringsmedium kan samtidigt innehålla såväl potentiella handlingar som färdiga elektroniska handlingar.

3. Utvecklingen av lagringsmediers lagringskapacitet har medfört att ett lagringsmedium kan innehålla en mycket stor mängd uppgifter samtidigt som det yttre utförandet kan vara mycket liten. Förlust av ett lagringsmedium som innehåller hemliga uppgifter kan potentiellt medföra konsekvenser i mycket stor omfattning. Jämförelsen med pappersdokument är talande - en förlust av *ett* lagringsmedium kan jämföras med en förlust av tusentals pappersdokument. Bild 12:1 illustrerar hur mycket enkelsidigt papper som motsvarar ett USB-minne på 2 GB.

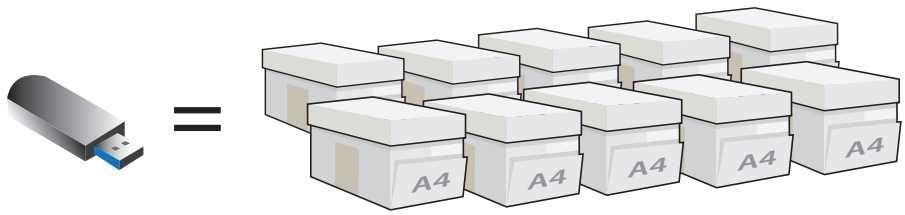


Bild 12:1 - Ett Word-dokument på tio sidor och med två bilder kan vara 800 kB stort. Ett USB-minne på 2 GB kan då innehålla 2 500 sådana dokument. Det motsvarar tio lådor med skrivarpapper eller 25 000 enkelsidiga A4-sidor.

4. En säkerhetskopia är undantagen från att vara en allmän handling.[255] Med *säkerhetskopia* avses här ett lagringsmedium vars syfte är att kunna återskapa information som har gått förlorad i ett IT-system (avsnitt 16).

254 Sidorna 33-34, Allmänna handlingar i elektronisk form – offentlighet och integritet (SOU 2010:4).
255 2 kap. 10 § andra stycket TF.

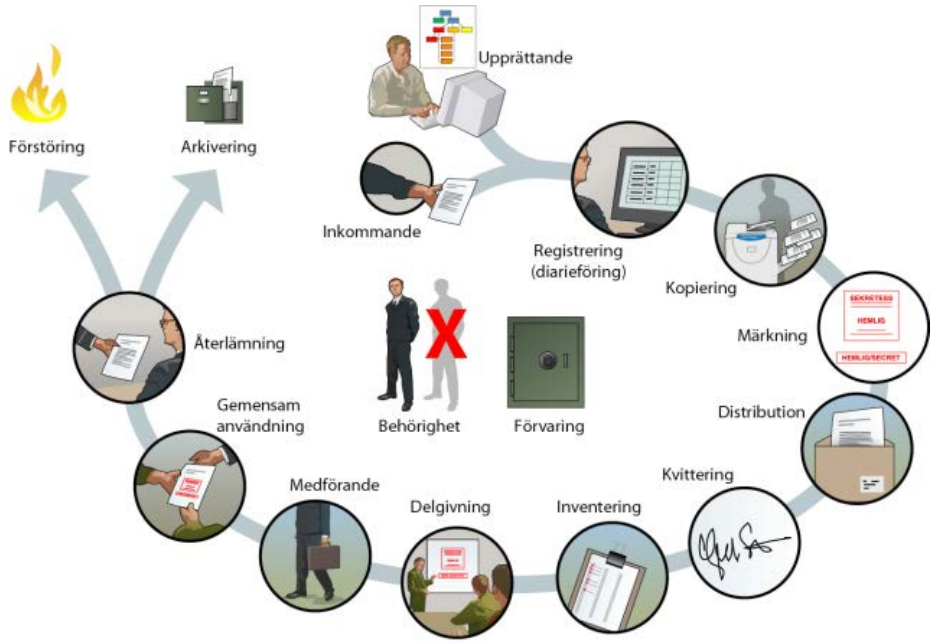


Bild 12:2 - En handlings livscykel och skyddsåtgärder under livscykeln gäller även för ett lagringsmedium.

I IT-system kan lagringsmedier användas för olika ändamål. Säkerhetsskyddet behöver anpassas för dessa ändamål. Föreskrifterna får tillämpas olika för lagringsmedier som är avsedda för:

- *personligt eller gemensamt tjänstebruk* respektive
- *drift eller säkerhetskopiering.*

Med *lagringsmedium som är avsett för personligt eller gemensamt tjänstebruk* avses ett lagringsmedium som används av en eller flera personer för behandling av hemliga uppgifter, till vilka personen eller personerna är behöriga, samt att personen eller personerna ansvarar för förvaring av lagringsmediet. Ett exempel är en hårddisk som en person har tilldelats för att endast använda det i ett visst IT-system. Ett annat exempel är ett USB-minne som används gemensamt av flera personer för att överföra filer mellan flera IT-system.

Ett lagringsmedium som utgör en del av flera i en allmän handling, t.ex. en CD-ROM som bilaga till ett missiv i pappersformat, likställs här med ett *lagringsmedium som är avsett för personligt eller gemensamt tjänstebruk.*

Med *lagringsmedium som är avsett för drift eller säkerhetskopiering* avses ett lagringsmedium som ingår i ett IT-system och som används för att upprätthålla driften av det IT-system det ingår i och inte är avsett för personligt eller gemensamt tjänstebruk.

Med IT-system avses här även utvecklings-, test- och andra miljöer som inte direkt är avsedda för användare i en driftmiljö. Ett sådant lagringsmedium hanteras normalt enbart av tekniker som har till uppgift att upprätthålla drift av ett IT-system. Personal som hanterar ett sådant lagringsmedium är normalt heller inte behöriga att ta del av uppgifterna som lagras på lagringsmediet. Exempel på sådana lagringsmedier är hårddiskar som finns i en server, nätverksskrivare, digital kopiator, backupsystem eller ett lagringssystem. Det kan dock finnas lagringsmedier som är avsedda för drift eller säkerhetskopiering till vilka personalen är behöriga att ta del av de lagrade uppgifterna, t.ex. konfigurationsfiler.

Säkerhetsskydd för lagringsmedier ska, på motsvarande sätt som för hemliga handlingar, utformas så att de lagrade hemliga uppgifterna inte kommer obehöriga till del samt att eventuell förlust uppmärksammas.

I avsnitt 12.2.1-12.2.18 ges *förtydliganden* till vilket säkerhetsskydd som lagringsmedier ska ha. Avsnitten bör parallelläsas med motsvarande avsnitt i kapitel 9 som rör hemliga handlingar. Det huvudsakliga författningsstödet återfinns i portalparagrafen 7 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd.

12.2.1 Behörighet till lagringsmedier

Vilka personer som ska kunna *hantera* ett lagringsmedium styrs av:

- om personerna är behöriga att ta del av uppgifterna som lagras eller
- om personerna har till arbetsuppgift att hantera ett lagringsmedium utan att ta del av de lagrade uppgifterna (t.ex. IT-tekniker eller arkiv- och expeditionspersonal).

För ett *lagringsmedium som är avsett för personligt eller gemensamt tjänstebruk* ska föreskrifterna som beskrivs i kapitel 7 om behörighet att ta del av hemliga uppgifter och handlingar tillämpas.

För ett *lagringsmedium som är avsett för drift eller säkerhetskopiering* ska föreskrifterna som beskrivs i kapitel 7 om behörighet att ta del av hemliga uppgifter och handlingar endast tillämpas på lagringsmediet om personerna som hanterar det ska ta del av uppgifterna som lagras. Om personerna inte ska ta del av uppgifterna (t.ex. om en IT-tekniker endast har till arbetsuppgift att genomföra säkerhetskopiering) ska föreskrifterna om behörighet att ta del av hemliga uppgifter och handlingar inte tillämpas på ett sådant lagringsmedium.

För att en person ska vara behörig att *använda eller ta del av uppgifter i ett IT-system* ska chefen för organisationsenheten först ha fattat ett beslut.[256] Beslutet får delegeras. En person som har ett lagringsmedium i syfte att använda eller ta del av uppgifterna i ett IT-system får endast göra det om chefen har beslutat en sådan behörighet. Se även avsnitt 18.3.6 om behörighet i IT-system.

12.2.2 Registrering av lagringsmedier

Ett lagringsmedium som är avsett för hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre ska registreras i ett register.[257] Syftet med registreringen är att upprätthålla kontrollen över lagringsmediet under dess livscykel, från att det har förberetts för användning till dess att det har förstörts. Ett sådant register utgör underlag för inventering av lagringsmedier.

För ett *lagringsmedium som är avsett för personligt eller gemensamt tjänstebruk* bör ett register för diarieföring av allmänna handlingar användas (se avsnitt 9.8.4). Det är lämpligt att expedition eller motsvarande används för registrering av sådana lagringsmedier.

För ett *lagringsmedium som är avsett för drift eller säkerhetskopiering* kan ett annat register än ett register för diarieföring av allmänna handlingar användas. För varje lagringsmedium bör det i ett sådant register framgå:

- unik identifieringsuppgift (t.ex. datum och ett löpnummer),
- vilken informationssäkerhetsklass som det har placerats i,
- för vilket ändamål det har skapats (t.ex. säkerhetskopiering),
- i vilket IT-system det ingår i,
- var det förvaras (t.ex. bandrobot B i rum 47 i byggnad C) samt
- om det har förkommit,
- vidtagna åtgärder (t.ex. överskrivning) för att säkerställa att hemliga uppgifter inte längre kan utläsas ur ett lagringsmedium som ska återanvändas[258], eller
- om det har förstörts.[259]

Ett register över lagringsmedier måste dessutom innehålla uppgifter som gör det möjligt att ta reda på i vilka IT-system som ett återanvänt lagringsmedium, som är placerat i informationssäkerhetsklass HEMLIG/SECRET eller HEMLIG/TOP SECRET, har använts i. Det är inte nödvändigt att ett lagringsmedium som återanvänds behåller det tilldelade unika identifieringsuppgiften för lagringsmediet.

256 7 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
257 2 kap. 19 § och 7 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd.
258 7 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd.
259 2 kap. 19 § Försvarsmaktens föreskrifter om säkerhetsskydd.

I sådana fall måste registret där lagringsmediet är registrerat även innehålla de tidigare identifieringsuppgifterna för lagringsmediet. Sådana uppgifter ska kunna användas för att i efterhand utreda händelser, t.ex. då ett lagringsmedium har förkommit eller hanterats med ett bristfälligt säkerhetsskydd. I avsnitt 12.5 beskrivs återanvändning av lagringsmedier.

Ett lagringsmedium brukar ofta ha ett serienummer och det är lämpligt att även serienummer framgår i ett register över lagringsmedier. Ett sådant serienummer får användas som unik identifieringsuppgift.

Då ett sådant lagringsmedium inte ska användas av en person, även om en IT-tekniker kommer att hantera det, behöver det ur säkerhetssynpunkt inte framgå vem som förvarar det.[259]

Då det är svårt att i förväg beakta den samlade informationsmängden som kan komma att lagras på ett lagringsmedium där uppgifter kontinuerligt kan tillföras (t.ex. en hårddisk eller ett USB-minne) *bör* även sådana lagringsmedier som är avsedda för eller som innehåller hemliga uppgifter i informationssäkerhetsklass HEMLIG/RESTRICTED registreras. Ett lagringsmedium som är avsett för eller som innehåller hemliga uppgifter i informationssäkerhetsklass HEMLIG/RESTRICTED där uppgifter inte kontinuerligt kan tillföras (t.ex. en icke omskrivningsbar CD-ROM) ska inte registreras för uppföljning av innehav, förlust och förstöring. I det fall ett sådant lagringsmedium utgör det enda exemplaret av en allmän handling ska det dock registreras i ett diarium för allmänna handlingar.

12.2.3 Kopiering av och utdrag ur lagringsmedier

På samma sätt som det ska finnas rutiner som ska förebygga att *svartkopior* av pappershandlingar uppstår (avsnitt 9.17.1) behöver det finnas motsvarande rutiner för lagringsmedier. Företeelsen svartkopia är lätt att förstå när det är fråga om pappershandlingar. Behovet av skyddsåtgärder för lagringsmedier är inte alltid analogt med behovet för pappershandlingar. I vissa fall kan en rutin som är lämplig för pappershandlingar vara meningslös för lagringsmedier. Rutiner för kopiering av eller utdrag ur lagringsmedier kan därför behöva utformas på ett annat sätt än för pappershandlingar.

Ett kontinuerligt utdrag ur ett lagringsmedium kommer att ske om det är *avsett för personligt eller gemensamt tjänstebruk* och ingår i ett IT-system för en användares huvudsakliga lagring och behandling av hemliga uppgifter. Att för en sådan normal användning av ett lagringsmedium besluta om utdrag ur lagringsmediet är inte meningsfullt (se även exempel 12:2 om säkerhetskopiering).

I fråga om kopiering av ett lagringsmedium som är *avsett för personligt eller gemensamt tjänstebruk,* och som inte ingår i ett IT-system för en användares huvudsakliga lagring och behandling av hemliga uppgifter, bör samma rutiner som för hemliga handlingar i pappersform användas (exempel 12:1).

Exempel 12:1

Expeditionspersonal har fått i uppdrag att kopiera en allmän handling som är hemlig och som är placerad i informationssäkerhetsklass HEMLIG/SECRET i ytterligare ett exemplar. En CD-ROM ingår som bilaga i pappershandlingen. Det finns beslutade och dokumenterade rutiner som innebär att en chef ska besluta om kopieringen. Enligt rutinerna ska expeditionspersonalen se till att kopieringen genomförs så att det nya exemplaret registreras.

Kopieringen av CD-ROM:en täcks in av beslutet att kopiera handlingen. Ett ytterligare beslut för att få kopiera CD-ROM:en behöver inte fattas.

För ett lagringsmedium *som är avsett* för drift eller säkerhetskopiering är rutinerna för kopiering av eller utdrag ur hemliga handlingar i pappersform inte meningsfulla då det används i det IT-system det är avsett för. Det skulle kontinuerligt omfatta samtliga uppgifter som lagras på ett sådant lagringsmedium. Det betyder inte att ett sådant lagringsmedium får hanteras utan säkerhetsskydd i övrigt, t.ex. vad gäller registrering, märkning och inventering.

Exempel 12:2

I ett IT-system som är godkänt för behandling av hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL genomförs säkerhetskopiering. Då säkerhetskopieringen genomförs periodiskt uppstår det hela tiden nya kopior av IT-systemets elektroniska handlingar. Dessa kan sägas vara utdrag ur lagringsmedier som kopieras till säkerhetskopiorna. Spårbarhet i form av exemplarhantering (registrering av ytterligare exemplar i det register handlingen är diarieförd) är inte meningsfull i fråga om de säkerhetskopierade elektroniska handlingarna. Säkerhetskopian är inte en svartkopia. Det är ur säkerhetssynpunkt mycket viktigare att genom registrering och inventering upprätthålla kontroll över de lagringsmedier som används för säkerhetskopiering.

När ett lagringsmedium, som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre, *spegelkopieras* för en

forensisk undersökning ska det finnas ett beslut om kopieringen. Spegelkopian ska hanteras med säkerhetsskydd, t.ex. vad gäller registrering, märkning och inventering.

Krav på *anteckning vid kopiering och utdrag* (avsnitt 9.17.1) gäller även för kopiering mellan två lagringsmedier som avses innehålla eller som innehåller hemliga uppgifter och *som är avsedda* för *personligt eller gemensamt tjänstebruk*. I vilka fall kopieringen ska dokumenteras framgår av följande tabell där anger att anteckning om kopiering ska ske.[260] Se även exempel 12:3.

	Dokumenterad kopiering av en handling mellan två lagringsmedier som är avsedda för personligt eller gemensamt tjänstebruk	
	Allmän handling	Arbetshandling
H/TS	X	
H/S	X	
H/C	X	
H/R		

Exempel 12:3

Stefan och Eva arbetar tillsammans i ett projekt. Stefan har en bärbar dator för att arbeta med en rapport i projektet. Rapporten innehåller hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/SECRET. Stefan kopierar rapporten till Evas USB-minne då även Eva ska arbeta med rapporten innan den kan fastställas.

Stefan behöver inte anteckna att kopiering av rapporten till Evas USB-minne har gjorts då rapporten fortfarande är under utarbetande och inte har nått sin slutgiltiga utformning, rapporten är inte en allmän handling.

En säkerhetsfunktion för säkerhetsloggning i ett IT-system kan användas för att automatiskt registrera kopiering eller utdrag ur en allmän handling som är en hemlig handling och som är placerad i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre.[261] Det måste i sådana fall vara möjligt att i efterhand ta reda på vilka handlingar det är fråga om. I övriga fall antecknas kopieringen eller utdraget manuellt av användaren i ett register eller en liggare.

260 2 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd.
261 2 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Kopiering av eller utdrag ur ett lagringsmedium som avses innehålla eller som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET får endast genomföras efter medgivande av myndighetens chef eller den han bestämmer.[262] Beslutet kan alltså delegeras inom myndigheten och vara generellt utformat för att t.ex. omfatta ett visst IT-system, driftorganisation eller verksamhet. I Försvarsmakten fattas ett sådant beslut av chef för en organisationsenhet eller den han eller hon bestämmer.[263]

I de fall det inte bedöms vara meningsfullt att ha rutiner som innebär att kopiering av eller utdrag ur ett lagringsmedium ska beslutas eller dokumenteras, hindrar det inte att sådana händelser registreras i en säkerhetslogg. Händelserna kan ändå vara av betydelse för säkerheten i och kring ett IT-system och ska då registreras i en säkerhetslogg för att i efterhand t.ex. kunna avgöra vem som har tagit del av de hemliga uppgifterna eller om de har exporterats ut ur ett IT-system.

12.2.4 Märkning av lagringsmedier

Även om märkningar såsom sekretessmarkering och informationssäkerhetsklass kan väcka uppmärksamhet om ett märkt lagringsmedium tappas bort överväger fördelarna med märkning. Märkning med *sekretessmarkering* (avsnitt 9.5.5) och *informationssäkerhetsklass* (avsnitt 6.4) ska anges på ett lagringsmedium som avses innehålla eller som innehåller hemliga uppgifter.[264] Om en sekretessmarkering inte får plats får den utelämnas, t.ex. på ett USB-minne. Det är då lämpligt att märka ett lagringsmedium med *myndighetens namn* eller annan organisatorisk tillhörighet så att lagringsmediet vid en eventuell förlust kan återlämnas. Det bör poängteras att informationssäkerhetsklass alltid ska framgå på ett lagringsmedium som är avsett för lagring av hemliga uppgifter. Märkning med informationssäkerhetsklass får förkortas på ett lagringsmedium.

För att möjliggöra uppföljning av ett lagringsmedium ska det märkas med den *unika identifieringsuppgift* samt eventuellt exemplarnummer som det har fått i samband med registrering. Bild 12:3 visar ett exempel med märkning av en CD-ROM. Bild 12:4 visar ett exempel på märkning av ett USB-minne [referens 24].

262 2 kap. 9 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd.
263 1 kap. 4 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
264 2 kap. 1-2 §§ Försvarsmaktens föreskrifter om säkerhetsskydd.

Bild 12:3 - Exempel på märkning av en CD-ROM.

Bild 12:4 - Exempel på märkning av ett USB-minne.

Märkning med streckkod som innehåller ett lagringsmediums unika identifieringsuppgift får användas, under förutsättning att det finns ett godkänt IT-system med stöd för streckkodsläsare, för att underlätta registrering och inventering.

En märkning av ett lagringsmedium behöver inte vara utformad så att den inte kan avlägsnas av en person som hanterar lagringsmediet, en sådan egenskap är inte motiverad med hänsyn till att en person som innehar ett lagringsmedium kan kopiera innehållet. En långt viktigare egenskap är att texten på märkningen inte blir oläslig

eller att en etikett lossnar under användning. För ett lagringsmedium med små yttre dimensioner kan det vara lämpligt att använda märkning på en nyckelbricka eller motsvarande som fästs på lagringsmediet.

På en hårddisk som monteras i en *hårddiskkassett* ska märkningen alltid finnas på hårddisken och på kassetten. Märkningen på kassetten ska minst bestå av lagringsmediets informationssäkerhetsklass. En sekretessmarkering är således inte nödvändig på kassetten. Anledningen till denna dubbelmärkning är att hårddisken annars skulle sakna märkning om den monteras ur kassetten, t.ex. om en IT-tekniker behöver genomföra felsökning. Hårddiskkassetten ska om möjligt märkas så att märkningen är synlig när kassetten är införd i den utrustning den används i. Hårddiskkassetten bör även märkas med den *unika identifieringsuppgift* samt eventuellt exemplarnummer som hårddisken har fått i samband med registrering.

12.2.5 Märkning av fast monterade lagringsmedier som är avsedda för drift eller säkerhetskopiering

Vissa *fast monterade lagringsmedier som är avsedda för drift eller säkerhetskopiering* är inte möjliga att märka med sekretessmarkering, informationssäkerhetsklass och identifieringsuppgifter. Om sådana lagringsmedier inte kan märkas ska istället märkningen placeras synligt och i så nära anslutning till lagringsmedierna som möjligt. Om det är möjligt ska utrustningen märkas så att det klart framgår för en person som befinner sig vid utrustningen att utrustningen innehåller lagringsmedier som är placerade i en informationssäkerhetsklass. I det fall utrustningen inte kan märkas får märkningen placeras på dörr eller lucka till det utrymme där utrustningen är placerad. Märkningen ska minst bestå av informationssäkerhetsklass.

När ett sådant lagringsmedium monteras ur utrustningen, t.ex. för service eller avveckling, ska det minst märkas med informationssäkerhetsklass. Om lagringsmediet åter ska monteras fast i en utrustning får märkningen tas bort vid monteringen.

12.2.6 Distribution av lagringsmedier

Föreskrifterna om distribution av hemliga handlingar som beskrivs i avsnitten 9.20.1, 9.21.1, 9.21.2 och 9.22.1 gäller även för distribution av lagringsmedier som avses innehålla eller som innehåller hemliga uppgifter.

12.2.7 Kvittering vid mottagande av lagringsmedier

Mottagande av ett *lagringsmedium som är avsett för personligt eller gemensamt tjänstebruk* och som är placerat i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre ska kvitteras. Det är lämpligt att rutiner för kvittering av hemliga handlingar används (se avsnitt 9.9).

Riksarkivet har meddelat föreskrifter om gallring som innebär att kvitton för lagringsmedier som innehåller eller är avsedda att innehålla hemliga uppgifter ska gallras efter 10 år. Kvitton för utlämning av lagringsmedier som innehåller eller är avsedda att innehålla kvalificerat hemliga uppgifter ska gallras efter 25 år. Föreskrifterna om sådan gallring gäller för myndigheter under försvarsdepartementet.[265]

Ett *lagringsmedium som är avsett för drift eller säkerhetskopiering* ska inte kvitteras vid mottagande då det inte är avsett för personligt eller gemensamt tjänstebruk. En IT-tekniker som hanterar sådana lagringsmedier gör det normalt under en begränsad tid, t.ex. i samband med installation eller underhåll av utrustning. Det är därför inte motiverat att den enskilde teknikern ska kunna hållas ansvarig för ett lagringsmedium som denne inte har rådighet över. En ordning där chef för en verksamhet kvitterar sådana lagringsmedier är inte heller lämplig då han eller hon inte heller har rådighet över lagringsmedierna.

12.2.8 Inventering av lagringsmedier

Ett *lagringsmedium som är avsett för personligt eller gemensamt tjänstebruk* och som är placerat i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET och som inte är arkiverat ska i Försvarsmakten inventeras minst en gång per år.[266] Det är lämpligt att rutiner för inventering av hemliga handlingar används (avsnitt 9.16.1).

Ett *lagringsmedium som är avsett för drift eller säkerhetskopiering* och som är placerat i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET och som inte är arkiverat ska i Försvarsmakten inventeras minst en gång per år.[266]

Alla lagringsmedier, inklusive arkiverade, som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET ska i Försvarsmakten inventeras minst en gång per år.[267] Inventeringen ska utföras av två inventeringsförrättare.[268]

En inventering av lagringsmedier som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre ska protokollföras av varje myndighet.[269] Det är lämpligt att rutiner för protokollföring vid inventering av hemliga handlingar används. *Märkning med streckkod* som innehåller ett lagringsmediums unika identifieringsuppgift, tilldelad vid registrering eller tillverkarens serienummer, får användas för att underlätta inventering.

265 2 § Riksarkivets föreskrifter om gallring hos myndigheter under Försvarsdepartementet.
266 2 kap. 13 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
267 2 kap. 12 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
268 2 kap. 14 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
269 2 kap. 21 § Försvarsmaktens föreskrifter om säkerhetsskydd.

12.2.9 Inventering av fast monteragde lagringsmedier som är avsedda för drift eller säkerhetskopiering

Krav på inventering av ett lagringsmedium som är placerat i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre gäller även ett lagringsmedium som är fast monterat (t.ex. en hårddisk i en server). [266] [267] [268] [269] Inventering av sådana lagringsmedier kan ske manuellt eller automatiserat. Ett lagringsmedium har oftast ett serienummer som är åtkomligt för avläsning genom det gränssnitt som det är anslutet med. I IT-system kan det vara lämpligt att använda tekniska funktioner för att läsa av serienummer på fast monterade lagringsmedier för att genomföra inventeringen. En sådan automatiserad inventering kan då ske kontinuerligt istället för med den periodicitet som myndigheten har beslutat i fråga om hemliga handlingar (avsnitt 9.16.1.).

I de fall det inte är möjligt att manuellt eller genom tekniska funktioner genomföra en inventering av *fast monterade lagringsmedier som är avsedda för drift eller säkerhetskopiering* får inventeringen av flera sådana lagringsmedier genomföras samlat. För att kunna genomföra en *samlad inventering* måste utrustningen vara förseglad (t.ex. med en plombering) på ett sådant sätt att det inte är möjligt att komma åt ett lagringsmedium utan att förseglingen bryts. Förseglingen måste vara så beskaffad att det är möjligt att genom okulär besiktning upptäcka om en försegling har ersatts med en ny försegling (t.ex. numrerad plombering). Då utrustningen förbereds för drift registreras vilka lagringsmedier som är fast monterade i utrustningen. Varje sådan utrustning ges en unik identifieringsuppgift som korresponderar mot identifieringsuppgifterna för varje fast monterat lagringsmedium. Vid en inventering kontrolleras förseglingen okulärt varefter utrustningens identifieringsuppgift antecknas i ett inventeringsprotokoll. De fast monterade lagringsmedierna i utrustningen är då inventerade. Ingrepp i en utrustning som innebär att förseglingen bryts bör ske av två personer i förening (tvåhandsfattning) till dess att utrustningen har förseglats på nytt.

Att använda säkerhetsfunktionen säkerhetsloggning för att upptäcka om ett lagringsmedium har monteras ur en utrustning kan inte ersätta en manuell eller automatiserad inventering. Skälet till detta är att det är fråga om två olika skyddsåtgärder där säkerhetsloggningen kompletterar skyddsåtgärden inventering.'

12.2.10 Förvaring av lagringsmedier

Föreskrifterna om förvaring av hemliga handlingar som beskrivs i avsnitt 9.11 gäller även för ett lagringsmedium som avses innehålla eller som innehåller hemliga uppgifter.

Ett *lagringsmedium som är avsett för personligt eller gemensamt tjänstebruk* ska förvaras av den person som har kvitterat det. Ett sådant lagringsmedium får även användas gemensamt av flera personer om detta har beslutats (se avsnitt 9.15).

Ett *lagringsmedium som är avsett för drift eller säkerhetskopiering* bör förvaras av den person som har till arbetsuppgift att hantera det, när det inte är monterat i den utrustning som det ska användas i. I de fall flera personer har till arbetsuppgift att hantera ett sådant lagringsmedium (t.ex. då flera tekniker har till arbetsuppgift att genomföra säkerhetskopiering) ska i Försvarsmakten beslut om *gemensam användning* fattas (se avsnitt 9.15).

12.2.11 Samförvaring av lagringsmedier

Föreskrifterna om samförvaring som beskrivs i avsnitt 9.12.1 gäller även för lagringsmedier som avses innehålla eller som innehåller hemliga uppgifter.

12.2.12 Medförande av lagringsmedier

Föreskrifterna om medförande av hemliga handlingar som beskrivs i avsnitt 9.13.1 gäller även för lagringsmedier som avses innehålla eller som innehåller hemliga uppgifter.

Med hänsyn till att ett lagringsmedium kan innehålla en mycket stor mängd hemliga uppgifter bör uppgifterna på ett lagringsmedium som ska medföras om möjligt krypteras. En sådan kryptering får endast ske med ett signalskyddssystem som har godkänts av chefen för MUST eller den han eller hon bestämmer.[270]

12.2.13 Gemensam användning av lagringsmedier

Föreskrifterna om gemensam användning av hemliga handlingar som beskrivs i avsnitt 9.15 gäller även för lagringsmedier som avses innehålla eller som innehåller hemliga uppgifter.

12.2.14 Återlämning av lagringsmedier

Ett lagringsmedium som inte längre behövs, t.ex. vid befattningsbyte eller när en anställning upphör ska återlämnas till arbetsgivaren.

Normalt ska ett *lagringsmedium som är avsett för personligt eller gemensamt tjänstebruk* återlämnas till den expedition där innehavaren har kvitterat det. På expeditionen antecknas ett lagringsmedium som återlämnats i det register där det är registrerat. Det tas därefter om hand för förstöring om det inte ska arkiveras.

I de fall en expedition eller motsvarande används för registrering och utlämning av *lagringsmedier som är avsedda för drift eller säkerhetskopiering* återlämnas sådana lagringsmedier till expeditionen. I de fall t.ex. en IT-driftorganisation svarar för regist-

270 13 § andra stycket säkerhetsskyddsförordningen och 9 § Försvarsmaktens interna bestämmelser om signalskyddstjänsten.

rering av sådana lagringsmedier kan IT-driftorganisationen internt hantera återlämningen så att ett lagringsmedium antecknas som återlämnat. Det tas sedan om hand för förstöring om det inte ska arkiveras.

I de fall en expedition eller motsvarande inte används för registrering och utlämning av *lagringsmedier som är avsedda för drift eller säkerhetskopiering* är det ur säkerhetssynpunkt av väsentlig betydelse att en eventuell förlust av ett lagringsmedium verkligen uppmärksammas. De personer som ansvarar för ett register över sådana lagringsmedier ska därför inte vara samma personer som hanterar lagringsmedierna för drift eller säkerhetskopiering. På detta sätt uppnås en självständighet för de personer som ska kontrollera existensen av ett registrerat lagringsmedium.

12.2.15 Arkivering av lagringsmedier

Riksarkivet har endast meddelat funktionskrav på lagringsmedier vilket innebär att några specifika typer av lagringsmedier inte har pekats ut för arkivering. För bevarande av elektroniska handlingar finns föreskrifter i

- Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling) samt
- Riksarkivets föreskrifter och allmänna råd om tekniska krav för elektroniska handlingar (upptagningar för automatiserad behandling).

Det är nödvändigt att uppmärksamma föreskrifterna under utveckling och anskaffning av ett IT-system så att åtgärder för bevarande av elektroniska handlingar kan uppmärksammas innan IT-systemet driftsätts.

12.2.16 Förstöring av lagringsmedier

> *Förstöring av hemliga handlingar eller av materiel som innehåller hemliga uppgifter skall ske så att åtkomst och återskapande av uppgifterna omöjliggörs.*
>
> *Förstöring av sådana hemliga handlingar och sådan materiel som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller högre skall dokumenteras utom såvitt avser karbonpapper, karbonband och färgband.*
>
> 2 kap. 22 § Försvarsmaktens föreskrifter om säkerhetsskydd

Med *materiel som innehåller hemliga uppgifter* avses bl.a. lagringsmedium. Uppgifter som har lagrats på ett lagringsmedium kan i vissa fall, beroende på typ av lagringsme-

dium och använd teknik, återskapas trots att åtgärder har vidtagits för att förhindra läsning.

MUST har beslutat om ett direktiv för förstöring av lagringsmedier [referens 18]. Direktivet gäller alla slag av uppgifter som förekommer i Försvarsmakten. Direktivet anger hur lagringsmedier ska förstöras i Försvarsmakten så att uppgifter som lagrats inte längre kan läsas eller återskapas. I direktivet anges detaljerade krav på förstöringsmetoder och hur Försvarsmakten ska tillämpa de avtal om förstöring av lagringsmedier som Försvarets materielverk har tecknat med leverantörer.

Den tekniska utvecklingen inom området lagringsmedier är omfattande. Ett lagringsmedium kan innehålla en mycket stor mängd uppgifter. Mer kraftfulla datorer som samtidigt tar mindre plats innebär att utvecklingen av lagringsmedier har inneburit förändringar av lagringstäthet, komprimeringsalgoritmer och för magnetiska lagringsmedier även magnetstyrka.

Dagens lagringsmedier har en tätare lagring och mer komplicerade lagringsalgoritmer. Den tätare lagringen på en hårddisk innebär också högre krav på precision på ett läshuvuds placering vid skrivning och läsning. Att precisionen ökar medför att en överskrivning av ett spår sker utan att tolkningsbara informationsrester kan ligga kvar. Om det går att utläsa enstaka kvarvarande polariteter så är det mycket långt till att omtolka dessa enstaka polariteter till användbar information då det krävs dels specialiserad utrustning, dels kunskap om hårddiskens logiska uppbyggnad, komprimeringsalgoritmer samt vilken typ av data som har utlästs.

Gränssnitt och funktioner för hårddiskar följer standarder som möjliggör att information kan lagras på hårddisken utanför det lagringsutrymme som är synligt för användaren. Att hårddiskar innehåller styrprogramvara som står utanför Försvarsmaktens kontroll och kan innehålla skadlig kod är ytterligare en aspekt att beakta.

De metoder som används för förstöring av lagringsmedier som innehåller hemliga uppgifter måste ta höjd för att underrättelseaktörer kan ha utvecklat metoder som inte är allmänt kända, den framtida tekniska utvecklingen vad avser återskapande av information samt att sekretesstiden för uppgifter som omfattas av sekretess enligt 15 kap. 2 § OSL i vissa fall är högst 150 år.[271]

Sammantaget ger detta att metoder för förstöring av lagringsmedier som innehåller hemliga uppgifter placerade i högre informationssäkerhetsklasser är mer rigorösa än för lägre informationssäkerhetsklasser. Förstöring av lagringsmedier måste ske strukturerat så att enskilda lagringsmedium av misstag inte förstörs eller förstörs otillräckligt, t.ex. i de fall förstöring sker i flera steg.

271 4 § OSF.

Det ekonomiska värdet av ett lagringsmedium är i allmänhet mindre än det värde som de lagrade uppgifterna representerar och vars värde inte alltid kan mätas i ekonomiska termer.

Efter förstöring av ett lagringsmedium ska den ansträngning som krävs för att få fram uppgifterna vara mycket stor i förhållande till värdet och mängden uppgifter som har lagrats.

Godkända metoder för förstöring av lagringsmedier kan vara olika för olika informationssäkerhetsklasser. För en lägre informationssäkerhetsklass kan förstöringsalternativ för en högre informationssäkerhetsklass användas. För sekretessklassificerade uppgifter får även förstöringsalternativ för någon av informationssäkerhetsklasserna användas, t.ex. för att blanda ut lagringsmedier som är placerade i informationssäkerhetsklass.

Vid förstöring av lagringsmedier måste hänsyn tas till att olika slag av lagringsmedier har olika fysiska egenskaper. En förstöringsmetod som är lämplig för att förstöra en hårddisk kan vara direkt olämplig för ett optiskt lagringsmedium. Även utrustning som används för förstöring måste användas på rätt sätt så att de lagrade uppgifterna verkligen förstörs. Det finns t.ex. slipmaskiner för optiska lagringsmedier där en CD-, DVD- eller en Blu-ray-skiva måste förstöras olika då deras konstruktion med informationsbärande lager skiftar [referens 46].

12.2.17 Förstöring av lagringsmedier som innehåller kryptonycklar

För förstöring av lagringsmedier som innehåller kryptonycklar kan andra bestämmelser gälla. MUST har beslutat ett direktiv hur en CD-skiva som innehåller eller har innehållit kryptonycklar ska förstöras [referens 34].

12.2.18 Förlust av lagringsmedier

Förlust (t.ex. genom stöld eller oaktsamhet) av ett lagringsmedium som innehåller en hemlig uppgift ska säkerhetsrapporteras (kapitel 22). Säkerhetsrapportering ska även ske i de fall ett lagringsmedium som innehåller en hemlig uppgift inte kan visas upp vid en inventering (se kapitel 11 om åtgärder vid förlust och röjande).[272] Förhållandet att ett lagringsmedium som innehåller en hemlig uppgift och som i samband med avveckling av ett IT-system inte kan återfinnas ska säkerhetsrapporteras.

272 4 kap. 2 § Försvarsmaktens föreskrifter för Försvarsmaktens personal.

12.3 Anskaffning av lagringsmedier

Lagringsmedier som ska användas i Försvarsmakten ska anskaffas med de rutiner som finns för anskaffning av materiel och genomförs av de enheter som har till uppgift att genomföra anskaffning.

Med hänsyn till att ett lagringsmedium kan innehålla kolossala mängder uppgifter är det ur säkerhetssynpunkt inte lämpligt att, i fråga om lagringsmedier som är avsedda för *personligt eller gemensamt tjänstebruk*, använda ett lagringsmedium med alltför stor lagringskapacitet. Att ange en gräns i absolut tal för tillåten lagringskapacitet för ett sådant lagringsmedium är inte möjligt p.g.a. den tekniska utvecklingen.

Det finns sällan skäl att förse användare av IT-system med lagringsmedier som långt överskrider deras behov av att kunna lagra uppgifter. Vid anskaffning av ett lagringsmedium som är avsett för *personligt eller gemensamt tjänstebruk* bör från säkerhetssynpunkt ett lagringsmedium väljas som vid anskaffningstillfället har den lägsta lagringskapacitet som normalt är kommersiellt tillgängligt. Om verksamhetens behov av lagring överstiger en sådan lägsta kommersiellt tillgänglig lagringskapacitet bör ställningstagandet dokumenteras. Beslut om att anskaffa ett lagringsmedium med en lagringskapacitet som överstiger den lägsta kapaciteten bör fattas så långt ut i organisationen som möjligt, t.ex. av närmaste chef.

12.4 Hantering av lagringsmedier i IT-system

Frågan om hantering av ett lagringsmedium i ett IT-system kan ur IT-säkerhetssynpunkt delas upp i två delar:

1. Om *hantering av lagringsmediet är tillåten* med avseende på i vilken informationssäkerhetsklass det är placerat i.
2. Om det finns *ett erforderligt säkerhetsskydd* för att kunna ansluta lagringsmediet till IT-systemet.

För att få ansluta ett lagringsmedium måste båda delarna vara uppfyllda. Att ett lagringsmedium är placerat i samma eller lägre informationssäkerhetsklass än vad IT-systemet är godkänt för är inte tillräckligt för att få ansluta det till systemet. Det behöver även finnas ett skydd mot de hot som en anslutning av ett lagringsmedium medför. I de fall ett erforderligt säkerhetsskydd inte kan uppnås vid anslutning av ett lagringsmedium till ett IT-system får anslutning inte genomföras (avsnitt 13.1).[273]

De två delarna beskrivs i följande två avsnitt.

273 5 § första stycket säkerhetsskyddslagen.

12.4.1 Tillåten hantering med avseende på placering i informationssäkerhetsklass

Ett lagringsmedium som avses innehålla eller som innehåller hemliga uppgifter får endast hanteras i ett IT-system som uppfyller de krav som gäller för hantering av uppgifter i den högsta informationssäkerhetsklass som någon av uppgifterna på lagringsmediet kan komma att placeras i eller har placerats i.

7 kap. 4 § Försvarsmaktens föreskrifter om säkerhetsskydd

Med *hantering* avses här alla former av fysisk eller logisk anslutning oavsett om information överförs mellan det anslutna lagringsmediet och någon del av IT-systemet eller inte. Ett exempel är när ett flyttbart lagringsmedium ansluts till ett IT-system för att lagra eller läsa information.

Föreskriften innebär att ett lagringsmedium som t.ex. är avsett att innehålla eller som innehåller sådana hemliga uppgifter som har placerats i informationssäkerhetsklass HEMLIG/SECRET inte får hanteras i ett IT-system som är avsett för behandling av uppgifter som är placerade i en lägre informationssäkerhetsklass (HEMLIG/CONFIDENTIAL eller HEMLIG/RESTRICTED). Ett IT-system som är avsett för behandling av sådana uppgifter har inte ett säkerhetsskydd för att kunna hantera uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/SECRET. I bild 12:5 visas exempel på anslutning av olika lagringsmedier till ett IT-system.

I Försvarsmakten gäller föreskriften även för IT-system som är avsedda för behandling av utrikesklassificerade uppgifter.[274]

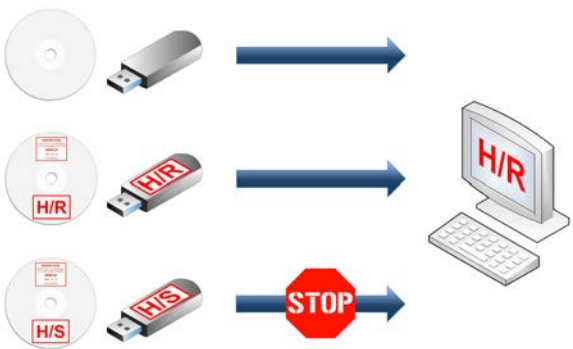


Bild 12:5 – Exempel på anslutning av olika lagringsmedier till ett IT-system som är godkänt för behandling av hemliga uppgifter som är placerade i informationssäkerhetsklass HEMLIG/RESTRICTED. Pilarnas riktning visar informationsflöden, i detta fall att uppgifter läses från lagringsmedierna till IT-systemet. Stoppskylten visar en otillåten anslutning med avseende på placering i informationssäkerhetsklass.

274 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Ett lagringsmedium som ansluts till ett IT-system som är godkänt för behandling av uppgifter som är placerade i en viss informationssäkerhetsklass medför inte att lagringsmediet placeras i den informationssäkerhetsklassen. Det är enbart då lagringsmediet *avses innehålla eller då det innehåller hemliga uppgifter* som lagringsmediet placeras i informationssäkerhetsklass (exempel 12:4).[275]

Exempel 12:4

Stina arbetar i ett IT-system som är godkänt för behandling av hemliga uppgifter som högst är placerade i informationssäkerhetsklass HEMLIG/RESTRICTED. Hon behöver kopiera några soldatreglementen från IT-systemet. Reglementena omfattas inte av sekretess enligt OSL. Till IT-systemet får USB-minnen anslutas.

Stina ansluter ett USB-minne till IT-systemet och kopierar soldatreglementen från IT-systemet till USB-minnet. USB-minnet är endast avsett för lagring av uppgifter som inte omfattas av sekretess enligt OSL.

Även om USB-minnet har hanterats i IT-systemet ändras inte dess informationsklassificering. Efter anslutningen till IT-systemet och kopieringen av reglementena till USB-minnet är USB-minnet fortfarande endast avsett för uppgifter som inte omfattas av sekretess enligt OSL.

Ett IT-system innehåller vanligtvis en blandning av uppgifter med avseende på sekretess och informationssäkerhetsklasser men även uppgifter som inte omfattas av någon sekretess. De verksamheter som ska stödjas av ett IT-system kan behöva använda uppgifterna utanför IT-systemet. På samma sätt kan det finnas ett verksamhetsbehov att tillföra uppgifter till ett IT-system. Överföring av uppgifter kan ske på ett lagringsmedium. När hemliga uppgifter ska lagras på ett lagringsmedium får det endast ske på ett lagringsmedium som är placerat i en informationssäkerhetsklass som är lika med eller högre än de överförda uppgifternas högsta informationssäkerhetsklass.[276] Bild 12:6 visar exempel på användning av lagringsmedier för överföring av uppgifter.

275 7 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd.
276 7 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Bild 12:6 – Exempel på användning av lagringsmedier för överföring av uppgifter. Lagringsmedierna är placerade i informationssäkerhetsklass HEMLIG/RESTRICTED och IT-systemet är godkänt för informationssäkerhetsklass HEMLIG/CONFIDENTIAL. Pilarnas riktning visar informationsflöden. De dubbelriktade pilarna visar att uppgifter från IT-systemet lagras på lagringsmedierna samt att uppgifter läses från lagringsmedierna till IT-systemet. Den enkelriktade pilen visar att uppgifter från IT-systemet lagras på lagringsmedierna. SK är en förkortning för sekretessklassificerade uppgifter. Stoppskylten visar en otillåten överföring med avseende på lagringsmediernas placering i informationssäkerhetsklass.

12.4.2 Säkerhetsskydd vid anslutning av flyttbara lagringsmedier

Säkerhetsskydd för lagringsmedier beskrivs i avsnitt 12.2, t.ex. vilka krav som gäller för förvaring av ett lagringsmedium. Detta avsnitt beskriver säkerhetsskydd för anslutning av flyttbara lagringsmedier till IT-system.

Ett flyttbart lagringsmedium som ansluts till ett IT-system är en del av IT-systemets informationsutbyte med andra IT-system. Hur mycket ett IT-system är exponerat, och därmed möjligt för en aktör att påverka systemet, är bl.a. beroende på informationsutbyte med flyttbara lagringsmedier (se avsnitt 2.5 i bilaga 1 till KSF 3.0 [referens 44] om exponeringsnivåer). Informationsöverföring med hjälp av flyttbara lagringsmedier används t.ex. mellan två IT-system där det i övrigt inte finns någon fysisk anslutning (s.k. luftgap).

Anslutning av ett flyttbart lagringsmedium till ett IT-system är ett tillfälle för en underrättelseaktör att påverka IT-systemet, t.ex. genom att införa skadlig kod eller för att obemärkt läsa ut hemliga uppgifter (s.k. exfiltrering). Vanligt förekommande antivirusprogram kan inte skydda mot skadlig kod som har utvecklats för att undgå detektering och utgör därför inte ett tillräckligt skydd. Informationsförluster till följd av att en behörig användare avsiktligt har kopierat hemliga uppgifter till ett flyttbart lagringsmedium är ytterligare ett hot som säkerhetsskyddet ska förebygga (se även avsnitt 13.1 om säkerhetsskydd i och kring IT-system). Att enbart konstruera skyddet kring anslutning av lagringsmedier på administrativa bestämmelser är normalt inte tillräckligt ur säkerhetssynpunkt.

Informationsöverföring med flyttbara lagringsmedier är således i grunden osäker. Detta innebär att ett IT-system som är avsett för behandling av hemliga uppgifter inte får konstrueras så att flyttbara lagringsmedier godtyckligt kan anslutas till IT-systemet.[277] Behovet av säkerhetsskydd i ett IT-system där överföring av hemliga uppgifter genom flyttbara lagringsmedier är nödvändig måste uppmärksammas i en säkerhetsmålsättning för IT-systemet (avsnitt 14.1). Vilka typer av anslutningar som är tillåtna för ett visst IT-system måste även beskrivas i systemets ackreditering.

Ett erforderligt säkerhetsskydd för anslutning av ett flyttbart lagringsmedium uppnås genom en kombination av flera säkerhetsfunktioner, t.ex. behörighetskontroll, intrångsskydd, intrångsdetektering och säkerhetsloggning. Säkerhetsloggning är nödvändig för att i efterhand kunna rekonstruera händelseförlopp vid anslutning av flyttbara lagringsmedier, t.ex. vilka lagringsmedier som har anslutits och vilken information som har överförts.

Skyddsåtgärder för att minska risken för oönskad påverkan av ett IT-system eller obemärkt utläsning av hemliga uppgifter kan bl.a. bestå av:

- Att IT-systemet har en teknisk funktion som säkerställer att informationsflytt mellan systemet och ett flyttbart lagringsmedium strikt sker på användarens initiativ.
- Ej omskrivningsbara CD-ROM används istället för USB-minnen vid överföring av hemliga uppgifter mellan två IT-system.
- Möjligheten att ansluta flyttbara lagringsmedier till ett IT-system blockeras på logisk eller fysisk väg. In- och utläsning av uppgifter genomförs istället på särskilda enheter i IT-systemet och på ett sätt som ska förhindra en obehörig utläsning av hemliga uppgifter (t.ex. en rutin där en chefs godkännande krävs innan utläsning genomförs). Att blockera samtliga möjligheter att ansluta ett flyttbart lagringsmedium är inte motiverat för ett enanvändarsystem (avsnitt 13.9) då användaren har full kontroll över de behandlade uppgifterna.
- På teknisk väg endast tillåta anslutning av i förväg definierade lagringsmedier.

I det fall ett flyttbart lagringsmedium regelbundet används för att överföra hemliga uppgifter mellan två IT-system som är placerade i samma utrymme bör lagringsmediet inte tas med utanför utrymmet. En förlust av ett sådant lagringsmedium kan potentiellt innebära röjande av mycket stora mängder hemliga uppgifter.

277 5 § första stycket säkerhetsskyddslagen.

12.5 Återanvändning av lagringsmedier

Ett lagringsmedium som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/SECRET eller HEMLIG/TOP SECRET får inte återanvändas i ett IT-system som är avsett för behandling av hemliga uppgifter som är placerade i en lägre informationssäkerhetsklass.

7 kap. 5 § Försvarsmaktens föreskrifter om säkerhetsskydd

Föreskriften ger möjlighet att återanvända ett lagringsmedium som innehåller hemliga uppgifter och som är placerade i informationssäkerhetsklassen HEMLIG/SECRET i ett IT-system som är avsett för behandling av hemliga uppgifter och som är placerade i HEMLIG/SECRET eller HEMLIG/TOP SECRET. Lagringsmediet får följaktligen återanvändas i ett IT-system som har samma eller ett starkare säkerhetsskydd än det ursprungliga IT-systemet. Mediet behåller sin informationssäkerhetsklass till dess att det är förstört på så sätt att åtkomst och återskapande av uppgifterna är omöjliggjord. Tidigare krav på att ett överskrivet lagringsmedium endast får återanvändas av personer som var behöriga till de uppgifter som fanns lagrade på mediet, har utgått [referens 39]. Villkor för återanvändning av hårddiskar i Försvarsmakten framgår i [referens 39].

Om ett återanvänt lagringsmedium som är placerat i informationssäkerhetsklass HEMLIG/SECRET eller HEMLIG/TOP SECRET förloras måste det vara möjligt att ta reda på i vilka IT-system som det har använts i. Det register som lagringsmediet är registrerat i (avsnitt 12.2.2) måste därför innehålla uppgifter som gör det möjligt att i efterhand konstatera detta.

Ett lagringsmedium som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/RESTRICTED eller HEMLIG/CONFIDENTIAL får återanvändas om myndigheten har vidtagit åtgärder för att säkerställa att inga hemliga uppgifter längre kan utläsas ur lagringsmediet. Sådana åtgärder skall dokumenteras.

7 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd

Föreskriften innebär även att ett lagringsmedium får återanvändas i sådana IT- system som inte är avsedda för behandling av hemliga uppgifter under förutsättning att myndigheten har vidtagit åtgärder för att säkerställa att inga hemliga uppgifter kan utläsas ur lagringsmediet, se bild 12:7.

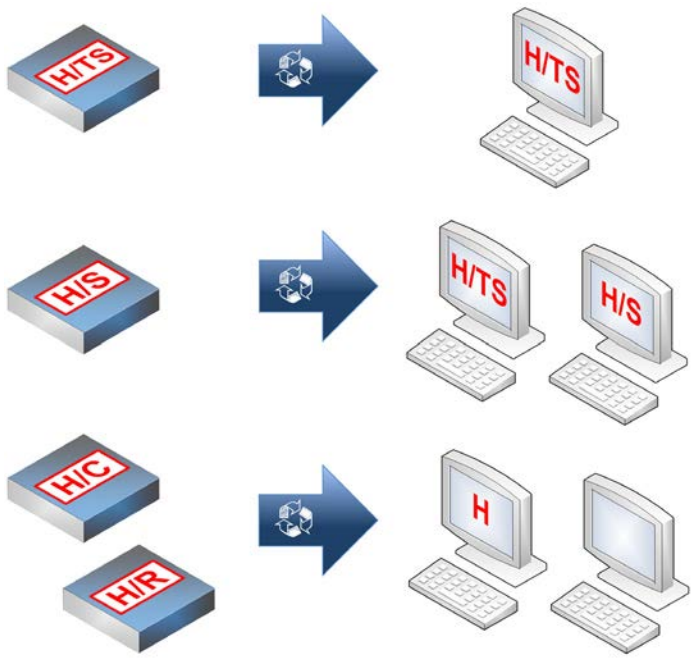


Bild 12:7 - Lagringsmedier får under vissa omständigheter återanvändas. Hur och i vilka fall beror bl.a. på vilken informationssäkerhetsklass som ett lagringsmedium är avsett att hantera.

För ett lagringsmedium som tidigare har varit placerat i informationssäkerhetsklass HEMLIG/RESTRICTED eller HEMLIG/CONFIDENTIAL är det inte nödvändigt att kunna ta reda på i vilka IT-system som det tidigare har använts i. Åtgärder som har vidtagits för att säkerställa att inga hemliga uppgifter längre kan utläsas ur lagringsmediet medför att en sådan spårbarhet inte behövs.

I [referens 39] beskrivs vilka produkter som ska användas för nämnda ändamål inom Försvarsmakten.

Överskrivning av ett lagringsmedium är ett sätt att säkerställa att de uppgifter som finns på lagringsmediet inte längre kan utläsas genom att verktyget skriver över den lagrade informationen med ny data. Överskrivningsverktyg används för att skriva över lagrade data från alla typer av magnetiska lagringsmedier såsom hårddiskar med roterande magnetiska skivor.

Överskrivning kan användas vid t.ex. återanvändning eller kassering av magnetiska lagringsmedier samt före förstöring av lagringsmedier. I det senare fallet är syftet att försvåra åtkomst till de uppgifter som förekommer på medierna om de skulle stjälas eller förkomma på något annat sätt.

Överskrivningsverktyg ska således användas för överskrivning av lagringsmedier som innehåller hemliga uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/RESTRICTED eller HEMLIG/CONFIDENTIAL innan medierna återanvänds. Efter godkänd överskrivning med ett godkänt överskrivningsverktyg bedöms sådana lagringsmedier inte längre innehålla hemliga uppgifter. Försvarsmakten anser dock att uppgifterna finns kvar på överskrivna lagringsmedier men i mikroskopiska rester. Det går alltså att på teknisk väg få fram fragment av uppgifterna. Ansträngningen för att få fram uppgifterna är dock mycket stor i förhållandet till värdet och mängden av uppgifterna, varför Försvarsmakten anser att åtgärder med överskrivning säkerställer att inga hemliga uppgifter längre kan utläsas ur lagringsmedierna.

En *degausser* är ett verktyg för att avmagnetisera digitala magnetiska lagringsmedier med hjälp av ett kraftigt magnetfält. En hårddisk som utsätts för ett kraftigt magnetfält blir både rensad på information och förstörd, p.g.a. att de data som styr uppstart av hårddisken också går förlorade. En degausser går att använda på alla typer av magnetiska lagringsmedier såsom magnetband, hårddiskar med roterande magnetiska skivor och floppydiskar. Magnetband som utsätts för sådan behandling kan dock, till skillnad från övriga nämnda magnetiska lagringsmedier, återanvändas.

Det är lämpligt att använda en degausser då en hårddisk gått sönder och någon överskrivning inte är möjlig att genomföra. Degausser ska användas om lagringsmediet innehåller uppgifter som omfattas av sekretess enligt OSL och rör rikets säkerhet, oavsett informationssäkerhetsklass.

Innan överskrivningsverktyg eller degausser används måste hänsyn tas till vad som föreskrivs i arkivlagen om bevarande och gallring av allmänna handlingar samt de myndighetsspecifika föreskrifter som har beslutats av Riksarkivet. Om ett lagringsmedium innehåller allmänna handlingar som inte får gallras får inte överskrivning eller degaussning genomföras.

Optiska lagringsmedier såsom CD eller DVD påverkas inte av båda dessa verktyg. Degausser kan inte påverka uppgifterna eftersom de lagras optiskt.

12.6 Utrikesklassificerade uppgifter

Ett lagringsmedium som är avsett att innehålla eller som innehåller utrikesklassificerade uppgifter ska i Försvarsmakten ha samma skydd som ett lagringsmedium som är avsett att innehålla eller som innehåller hemliga uppgifter.[278]

278 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

12.7 Sekretessklassificerade uppgifter

12.7.1 Skydd av lagringsmedier

> *Ett lagringsmedium som är avsett att innehålla eller som innehåller sekretessklassificerade uppgifter ska ha ett skydd som motsvarar det skydd som gäller för en sekretessklassificerad handling enligt Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade handlingar.*
>
> 3 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Föreskriften innebär att ett lagringsmedium som är avsett att innehålla eller som innehåller sekretessklassificerade uppgifter inte får hanteras i ett IT-system som inte är godkänt för behandling av sådana uppgifter. Sekretessklassificerade uppgifter får behandlas i IT-system som är avsett för hemliga och utrikesklassificerade uppgifter då sådana IT-system har ett skydd som går utöver skyddet som gäller för sekretessklassificerade uppgifter.

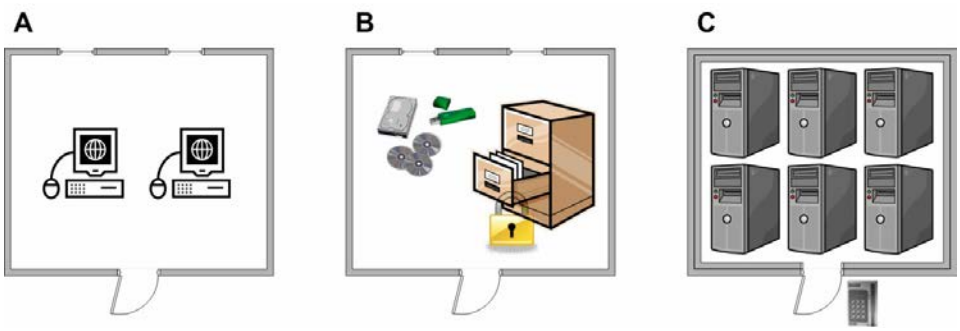


Bild 12:8 - Förvaring av lagringsmedier som innehåller sekretessklassificerade uppgifter.

Ett *fast monterat lagringsmedium*, t.ex. i en dator eller i en kopieringsmaskin, som innehåller sekretessklassificerade uppgifter och som är placerad inom Försvarsmaktens lokaler behöver av säkerhetsskäl inte förvaras i ett låst förvaringsutrymme som uppfyller krav på skyddsnivå 1 (A i bild 12:8).[279] Tillträdesskyddet i Försvarsmaktens lokaler bedöms vara tillräckligt för sådana lagringsmedier.

Till skillnad mot ett fast monterat lagringsmedium ska ett *flyttbart lagringsmedium*, t.ex. ett USB-minne, som innehåller sekretessklassificerade uppgifter och som inte står under uppsikt förvaras i ett låst förvaringsutrymme som uppfyller krav på skyddsnivå 1 (B i bild 12:8). Det finns i 3 kap. 11-17 §§ Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar krav på tillträdes-

279 Enligt bilaga i Försvarsmaktens föreskrifter om säkerhetsskydd.

skydd för utrymmen som innehåller växlar, korskopplingar och servrar samt datorhallar där det behandlas *betydande mängder* sekretessklassificerade uppgifter (C i bild 12:8) (avsnitt 13.4.3).

Den sammanlagda informationsmängden som finns på ett lagringsmedium behöver inte beaktas utom i de sällsynta fall där sammantagna sekretessklassificerade uppgifter bildar nya uppgifter som bedöms omfattas av sekretess och röra rikets säkerhet.[280]

Föreskriften innebär även att ett lagringsmedium som är avsett att innehålla eller som innehåller sekretessklassificerade uppgifter ska förses med sekretessmarkering (avsnitt 9.5).[281]

12.7.2 Återanvändning av lagringsmedier

Ett lagringsmedium som innehåller sekretessklassificerade uppgifter får återanvändas om åtgärder har vidtagits för att säkerställa att uppgifter inte längre kan utläsas ur lagringsmediet. Militära underrättelse- och säkerhetstjänsten i Högkvarteret ska fatta beslut om vilka åtgärder som krävs för att ett lagringsmedium ska få återanvändas.

3 kap. 2 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Föreskriften innebär att ett lagringsmedium får återanvändas i sådana IT-system som inte är avsedda för behandling av sekretessklassificerade uppgifter under förutsättning att organisationsenheten har vidtagit åtgärder för att säkerställa att inga sekretessklassificerade uppgifter kan utläsas ur lagringsmediet.

Överskrivningsverktyg får i Försvarsmakten användas för överskrivning av hårddiskar som innehåller sekretessklassificerade uppgifter [referens 39].

Åtgärderna som organisationsenheten vidtagit för att säkerställa att inga sekretessklassificerade uppgifter kan utläsas ur ett lagringsmedium behöver inte dokumenteras.

För ett lagringsmedium som tidigare innehållit sekretessklassificerade uppgifter är det inte nödvändigt att kunna ta reda på i vilka IT-system som det tidigare har använts i. Åtgärder som har vidtagits för att säkerställa att inga sekretessklassificerade uppgifter längre kan utläsas ur lagringsmediet medför att en sådan spårbarhet inte behövs.

280 Avsnitt 4.3.4 i H Säk Sekrbed A.
281 3 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

12.7.3 Kryptering av lagringsmedier

Det finns inget generellt författningskrav på att sekretessklassificerade uppgifter på ett lagringsmedium ska krypteras. En sådan skyddsåtgärd kan ändå vara lämplig för det fall att ett lagringsmedium förloras.

Mobila externa lagringsenheter är enligt auktorisationsbeslut [referens 43] lagringsmedier med USB eller Firewire som är avsett för hantering av sekretessklassificerade uppgifter. Auktorisationsbeslutet innehåller krav på egenskaper som gäller för mobila externa lagringsenheter och IT-system där sådana flyttbara lagringsmedier ska användas. Kraven i auktorisationsbeslutet innefattar bl.a. att sådana enheter ska ha ”stöldskydd/lässkydd i form av kommersiell kryptering, minst AES 256 eller motsvarande.”

12.7.4 Förstöring av lagringsmedier

> *Förstöring av ett lagringsmedium som får förstöras ska ske så att åtkomst och återskapande av uppgifterna försvåras. Militära underrättelse- och säkerhetstjänsten i Högkvarteret ska fatta beslut om krav på åtgärder för förstöring.*
>
> 3 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Med *får förstöras* avses att ett lagringsmedium inte innehåller allmänna handlingar som ska bevaras enligt föreskrifter i arkivlagen.

Uppgifter som har lagrats på ett lagringsmedium kan i vissa fall, beroende på typ av lagringsmedium och använd teknik, återskapas trots att åtgärder har vidtagits för att förhindra läsning. Försvarsmakten har tagit fram ett direktiv där godkända metoder för förstöring av lagringsmedier framgår [referens 18].

Efter förstöring av ett lagringsmedium ska den ansträngning som krävs för att få fram uppgifterna vara mycket stor i förhållande till värdet och mängden uppgifter som har lagrats.

12.8 Gallring av handlingar som rör lagringsmedier

Föreskrifter om gallring av allmänna handlingar som rör säkerheten i och kring IT-system finns i Riksarkivets föreskrifter om gallring hos myndigheter under Försvarsdepartementet. I föreskriften framgår bl.a. följande gallringsfrister.

Slag av handling		Gallringsfrist
Förteckningar över lagringsmedier	Kvalificerat hemliga	25 år efter senaste anteckning
	Hemlig	10 år efter senaste anteckning
Kvitton vid utlämning av lagringsmedier	Kvalificerat hemliga	25 år
	Hemliga	10 år
	Övriga	När de inte behövs i verksamheten
Förstöringsrapporter (protokoll) över förstörda lagringsmedier	Kvalificerat hemliga	25 år efter senaste anteckning
	Hemlig	10 år efter senaste anteckning

13 IT-säkerhet

Med *IT-säkerhet* avses i denna handbok *åtgärder som syftar till att uppnå och vidmakthålla den nivå av säkerhet som bl.a. lagar, förordningar, Försvarsmaktens författningar, Försvarsmaktens informationssäkerhetspolicy, särskilda skrivelser och verksamhetens behov ställer på ett IT-system* (bild 13:1).

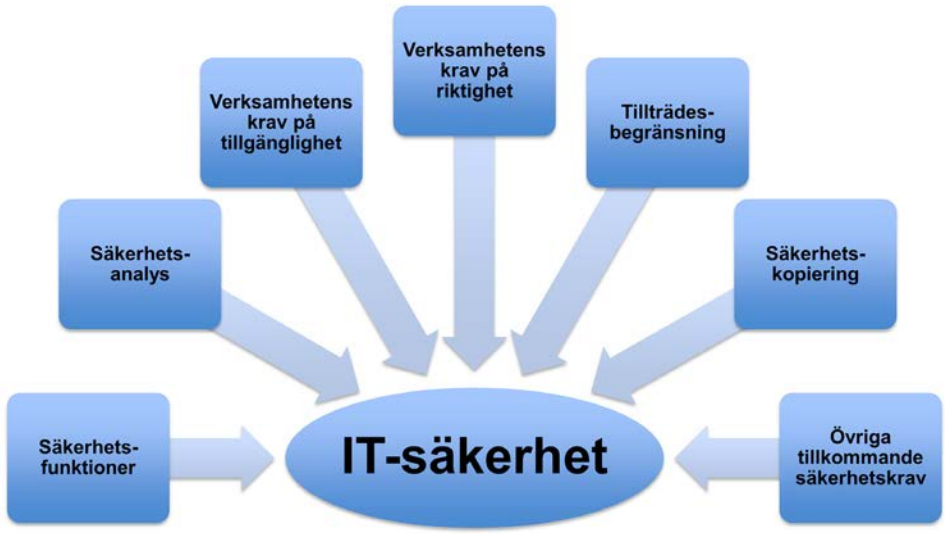


Bild 13:1 - Schematisk bild som visar olika slag av krav på IT-säkerhet. Bilden är inte uttömmande.

> *I detta kapitel avses med IT-system: system med teknik som hanterar och utbyter information med omgivningen.*
>
> 7 kap. 1 § 2 Försvarsmaktens föreskrifter om säkerhetsskydd

Ibland används begreppet informations- och kommunikationsteknik (IKT) (engelska: Information and Communication Technology, förkortas ICT) för att framhäva användningen av kommunikation i modern användning av informationsteknik (IT) (engelska: Information Technology). Begreppet IT-system omfattar i detta avseende IT *och* IKT. Exempel på ett IT-system är en dator, en router, ett nätverk av datorer, ett elektroniskt kommunikationsnät, ett sensorsystem för inhämtning av data, en programvara för ordbehandling, en digital kopiator eller en mobiltelefon. Avsikten är att begreppet IT-system ska vara heltäckande (bild 13:2).

Bild 13:2 – Datorer, skrivare, telefoner, elektroniska kopieringsmaskiner, läsplattor och telefonväxlar är exempel på IT-system. Även annan materiel kan vara IT-system.

I och med att IT-system enligt föreskriftens mening kan användas för allt från en ordbehandlare till hela nätverk av datorer måste skrivningar som ”varje IT-system” närmas med försiktighet. Det är t.ex. inte rimligt att varje enskild programvara i ett IT-system som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer förses med en säkerhetsfunktion för intrångsskydd. I stället får det omgärdande IT-systemet innehålla säkerhetsfunktionen intrångsskydd.

Med *utbyter information* avses inte enbart ett utbyte som sker med ett elektroniskt kommunikationsnät utan även andra former av enkel- eller dubbelriktat utbyte. Ett utbyte kan t.ex. ske elektromekaniskt (t.ex. genom ett tangentbord), genom utskrifter på en skrivare, presentation av information på en skärm eller genom en högtalare, taligenkänning och lagring av information på ett flyttbart lagringsmedium. Avsikten är att begreppet IT-system även i detta avseende ska vara heltäckande.

I dessa bestämmelser avses med IT-system: system med teknik som hanterar och utbyter information med omgivningen

2 § 1 Försvarsmaktens interna bestämmelser om IT-verksamhet

I dessa bestämmelser avses med IT-system: system med teknik som hanterar och utbyter information med omgivningen

1 kap. 6 § 1 Försvarsmaktens interna bestämmelser om IT-säkerhet

Begreppet IT-system används inte endast i fråga om IT-system som behöver ett säkerhetsskydd. I Försvarsmakten används begreppet IT-system oavsett för vilka slag av uppgifter som hanteras eller utbyts, därför är begreppet även definierat i Försvarsmaktens interna bestämmelser om IT-säkerhet.

Ett IT-system kan delas upp i *komponenter*. Komponenterna kan bestå av hård- eller mjukvara eller en kombination av sammansatta hård- och mjukvaror. En komponent, t.ex. en programvara, behöver normalt sättas samman med andra komponenter för att kunna användas. I KSF 3.0 används begreppet IT-säkerhetskomponent för en komponent som uppfyller eller bidrar till att uppfylla ett IT-säkerhetskrav på IT-systemet (IT-säkerhetsfunktionalitet). Försvarsmaktens författningar om IT-säkerhet gör ingen åtskillnad mellan ett IT-system och de komponenter som systemet består av. Detta hindrar inte att IT-säkerhetskrav på komponenter kravställs och att komponenter med erforderliga egenskaper anskaffas för att kunna användas i IT-system. Det finns ett behov av en tydligare begreppsmodell som överensstämmer med CIO styrande dokument (t.ex. Försvarsmaktens IT-styrmodell). Ett arbete kommer att initieras för att se över författningarna.

13.1 Säkerhetsskydd i och kring IT-system

I verksamhet där lagen gäller skall det säkerhetsskydd finnas som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter.

5 § första stycket säkerhetsskyddslagen

Säkerhetsskyddet i och kring ett IT-system behöver anpassas enligt föreskriften. Anpassningen avser inte vad som är möjligt att uppnå utan vilket säkerhetsskydd som behövs. Föreskriften innebär att varje myndighet måste avstå från ett IT-system om inte erforderligt säkerhetsskydd kan uppnås eller upprätthållas. På motsvarande sätt måste en myndighet avstå från en funktion i ett IT-system om inte erforderligt säkerhetsskydd för funktionen kan uppnås eller upprätthållas.

Vid utformningen av informationssäkerheten skall behovet av skydd vid automatisk informationsbehandling beaktas särskilt.

9 § säkerhetsskyddslagen

Lagstiftaren har 1996 genom föreskriften uttryckt vikten av att informationssäkerhet utformas med beaktande av de nya risker för förstörande eller röjande av hemliga uppgifter som finns i fråga om IT-system.[282] Innebörden av föreskriften har inte tappat i betydelse, tvärtom har den ökade digitaliseringen av informationstillgångar och verksamheters ökade beroende av IT-system medfört att de potentiella konsekvenserna är mer omfattande och allvarligare än tidigare.

Några exempel på sådana nya risker som avses i föreskriften är:

- Förekomsten av okända sårbarheter i ett IT-system som kan utnyttjas för att genomföra ett intrång i eller påverka ett IT-systems funktion.
- Då ett lagringsmedium kan innehålla stora mängder information kan konsekvenserna vid en förlust vara mycket stora.
- Svårigheten att förhindra intrång genom ett elektroniskt kommunikationsnät.
- Röjande av hemliga uppgifter som överförs utan godkänt signalskydd i ett elektroniskt kommunikationsnät.
- Obemärkt utläsning av hemliga uppgifter (s.k. exfiltrering) genom anslutning av ett flyttbart lagringsmedium.

Säkerhetsskydd ska bl.a. skydda mot spioneri, sabotage och andra brott som kan hota rikets säkerhet samt i övrigt skydda hemliga uppgifter.[283] Informationssäkerhet i och kring ett IT-system är i detta sammanhang ytterst en fråga om att upptäcka och förhindra att en behörig person (en s.k. insider) som går främmande makt tillhanda röjer hemliga uppgifter som behandlas i ett IT-system eller påverkar systemets funktion negativt. Den gränssättande aktören i detta sammanhang är andra staters underrättelsetjänster som kan ha vilja, förmåga och kapacitet att inhämta uppgifter genom angrepp på IT-system. Ett IT-system som är avsett för behandling av hemliga uppgifter ska därför utformas med krav på informationssäkerhet som kan möta en sådan aktörs ansträngningar. Normalt innebär detta att krav på informationssäkerhet för ett sådant IT-system är mer omfattande än andra IT-system i samhället. Detta innebär också att det normalt är nödvändigt med mer resurser för att uppfylla kraven jämfört med andra IT-system som inte omfattas av sådana krav.

282 Sidan 77, Säkerhetsskydd prop. 1995/96:129.
283 6 § säkerhetsskyddslagen.

En huvudprincip för säkerhetsskydd i och kring ett IT-system är vilken *tilltro* en myndighet ska sätta till ett påstående om säkerhetsegenskaper. En svårighet är inte enbart att påvisa en egenskap utan även att påvisa *avsaknaden* av *oönskade* egenskaper.

Informationssäkerhet i ett IT-system kan sägas vara en aspekt av en verksamhets kvalitetsarbete. Om en verksamhet har ett strukturerat kvalitetsarbete måste även informationssäkerheten tas om hand i kvalitetsarbetet, t.ex. vad gäller kravhantering, projektledning, test och dokumentation. Att hålla informationssäkerhetsarbetet utanför, t.ex. genom att inte låta utvecklare ta del av säkerhetskrav, medför vanligtvis en otillräcklig informationssäkerhet. Efter driftsättning av ett IT-system är vidmakthållande av informationssäkerheten i ett IT-system beroende av fungerande rutiner för bl.a. ändringshantering av hård- och mjukvaror. Informationssäkerhet i ett IT-system medför således indirekta krav på ordning och reda under utveckling, drift, förvaltning och avveckling av ett IT-system.

Informationssäkerhet i fråga om säkerhetsskydd ska förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs.[284] Det förebyggande syftet avser vare sig om röjande, ändring eller förstöring av hemliga uppgifter sker uppsåtligen eller av oaktsamhet.[285] Skyddsåtgärder för att reducera oavsiktliga skador på ett IT-system eller de behandlade uppgifterna är därför också säkerhetsskydd, t.ex. kontinuitetsplanering (avsnitt 14.6).

Om det för ett IT-system som är avsett för behandling av hemliga uppgifter finns motstridiga krav vad gäller önskvärd funktionalitet och krav på säkerhetsskydd har krav på säkerhetsskydd, med hänsyn till svårigheten att utforma en fullgod informationssäkerhet, företräde framför andra krav.[286]

13.2 Säkerhetsfunktioner i ett IT-system

Försvarsmakten och Säkerhetspolisen har definierat sju säkerhetsfunktioner för IT-system som är avsedda för behandling av hemliga uppgifter. En säkerhetsfunktion är en eller flera funktioner i ett IT-system som upprätthåller säkerheten enligt regler om hur uppgifter i IT-systemet ska skyddas.[287] I Försvarsmakten är dessa avsedda att skydda mot generella hot [referens 4, 5 och 23] för sådan verksamhet som bedrivs med stöd av IT. De sju säkerhetsfunktionerna är:

- Säkerhetsfunktionen för *behörighetskontroll*.[288]
- Säkerhetsfunktionen för *säkerhetsloggning*.[289]

284 7 § 1 säkerhetsskyddslagen.
285 Sidorna 26-27 och 74-75, Säkerhetsskydd prop. 1995/96:129.
286 5 § första stycket säkerhetsskyddslagen.
287 7 kap. 1 § 4 Försvarsmaktens föreskrifter om säkerhetsskydd.
288 7 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd.
289 7 kap. 11 § Försvarsmaktens föreskrifter om säkerhetsskydd.

- Säkerhetsfunktionen för *skydd mot röjande signaler*.[290]
- Säkerhetsfunktionen för *skydd mot obehörig avlyssning*.[290]
- Säkerhetsfunktionen för *intrångsskydd*.[291]
- Säkerhetsfunktionen för *intrångsdetektering*.[291]
- Säkerhetsfunktionen för *skydd mot skadlig kod*.[292]

Säkerhetsfunktionerna ska i Försvarsmakten även finnas i ett IT-system som är avsett för behandling av utrikesklassificerade uppgifter. Vissa säkerhetsfunktioner (t.ex. behörighetskontroll) ska i Försvarsmakten även finnas i IT-system som inte är avsett för behandling av hemliga eller utrikesklassificerade uppgifter (bild 13:3).

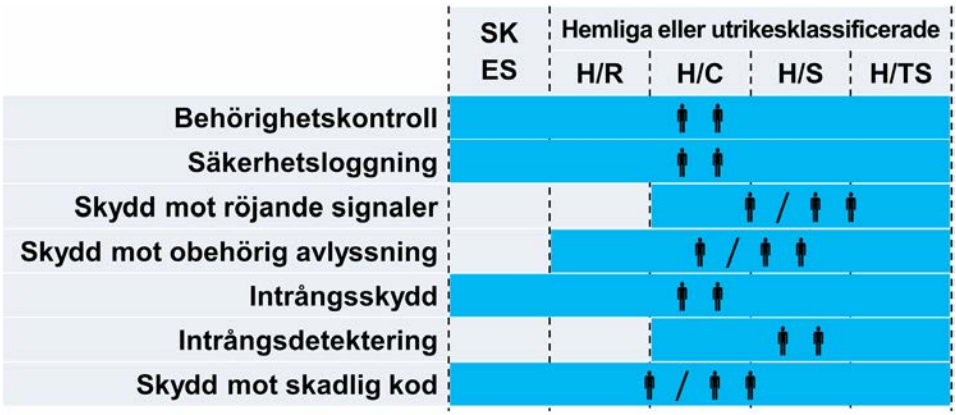


Bild 13:3 - Vilka säkerhetsfunktioner som ska finnas i ett IT-system i Försvarsmakten beroende på vilka uppgifter som IT-systemet är avsett att behandla samt om IT-systemet är avsett att användas av en (🧍) eller flera (🧍🧍) personer. SK i bilden avser sekretessklassificerade uppgifter. ES (ej sekretess) i bilden avser uppgifter som inte omfattas av sekretess enligt OSL.

En tillräcklig IT-säkerhet uppnås inte enbart med de sju säkerhetsfunktionerna då dessa inte definierar alla nödvändiga skyddsåtgärder. Ett exempel på detta är skyddsåtgärder med avseende på tillgänglighet där bl.a. Riksarkivets krav på säkerhetskopiering gäller (se kapitel 16). Ett annat exempel är om ytterligare behov av skyddsåtgärder har identifierats genom säkerhetsanalys. *Tillkommande säkerhetskrav*, utöver säkerhetsfunktionerna, beskrivs i avsnitt 13.3.

För Försvarsmakten har MUST beslutat krav på godkända säkerhetsfunktioner (KSF 2.0 och 3.0) [referenserna 7, 9 och 44]. Säkerhetsfunktionerna beskrivs utförligare i kapitel 18.

290 7 kap. 13 § Försvarsmaktens föreskrifter om säkerhetsskydd.
291 7 kap. 14 § Försvarsmaktens föreskrifter om säkerhetsskydd.
292 7 kap. 15 § Försvarsmaktens föreskrifter om säkerhetsskydd.

13.3 Tillkommande säkerhetskrav på ett IT-system

Ett tillräckligt skydd för ett IT-system uppnås inte enbart med de i föregående avsnitt angivna sju säkerhetsfunktionerna. För att uppnå ett tillräckligt skydd för ett IT-system krävs dessutom att krav på ytterligare skyddsåtgärder identifieras. Sådana krav benämns *tillkommande säkerhetskrav* i MUST krav på godkända säkerhetsfunktioner (KSF 3.0) [referens 44].

Tillkommande säkerhetskrav identifieras genom verksamhetsanalys (avsnitt 14.2), regelverksanalys (avsnitt 14.3) och säkerhetsanalys (avsnitt 14.4). Tillkommande säkerhetskrav dokumenteras i en IT-säkerhetsspecifikation (avsnitt 14.5) som ingår i en säkerhetsmålsättning (avsnitt 14.1) för ett IT-system.

Följande föreskrift är ett exempel på en källa för tillkommande säkerhetskravkrav för ett IT-system som är avsett för behandling av hemliga uppgifter. Andra exempel på tillkommande säkerhetskrav är:

- krav på skyddsåtgärder som rör behandling av personuppgifter och som inte bedöms omhändertas av säkerhetsfunktioner i ett IT-system,
- Riksarkivets krav för bevarande av elektroniska handlingar (avsnitt 12.2.15) och
- verksamhetens krav på tillgänglighet (avsnitt 14.2.2).

> *En hemlig uppgift i ett IT-system skall ha ett säkerhetsskydd som motsvarar det säkerhetsskydd som gäller för den informationssäkerhetsklass som uppgiften har placerats i.*
>
> 7 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd

Föreskriften är en portalparagraf för säkerhetsskydd för hemliga uppgifter som behandlas i ett IT-system. Av föreskriften följer att hemliga uppgifter i ett IT-system således ska hanteras på ett sådant sätt att säkerhetsskyddet motsvarar det säkerhetsskydd som gäller för hemliga handlingar. Även en hemlig handling som endast kan uppfattas med ett tekniskt hjälpmedel (t.ex. en elektronisk handling i ett IT-system) omfattas av föreskriften.

Föreskriften innebär att föreskrifterna i 2 kap. Försvarsmaktens föreskrifter om säkerhetsskydd ska tillämpas av en myndighet även i fråga om hemliga uppgifter i ett IT-system. I Försvarsmakten gäller dessutom att 2 kap. Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel även ska tillämpas på hemliga uppgifter i ett IT-system. Bild 13:4 visar en handlings livscykel och skyddsåtgärder

under livscykeln, dessa skyddsåtgärder gäller även för hemliga uppgifter som behandlas i ett IT-system.

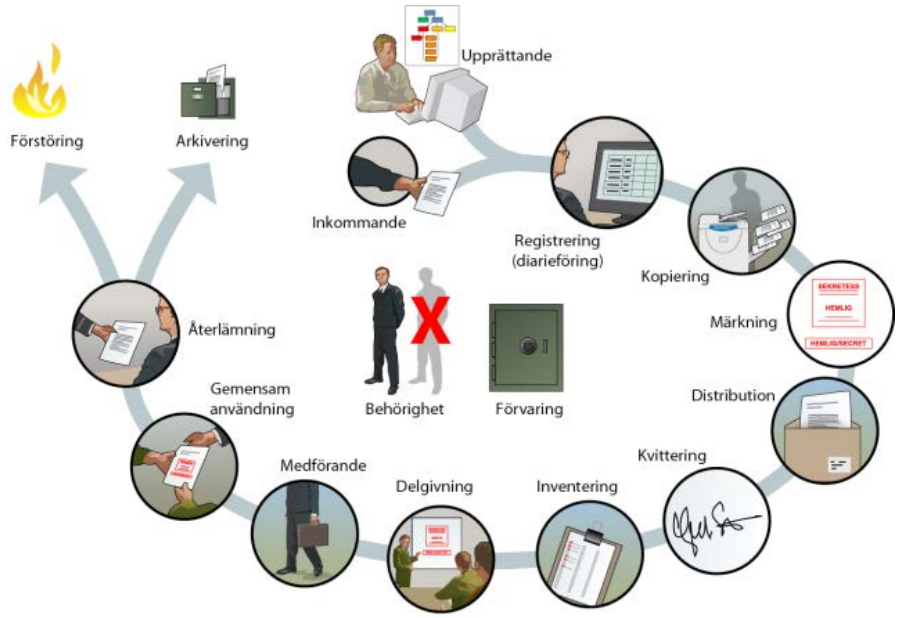


Bild 13:4 - En handlings livscykel och skyddsåtgärder under livscykeln gäller även för hemliga uppgifter i ett IT-system.

Föreskriften medför *tillkommande säkerhetskrav* på ett IT-system, t.ex. vad gäller märkning av hemliga handlingar i ett IT-system (sekretessmarkering, informationssäkerhetsklass m.m.) och exemplarhantering vid utskrift (se även avsnitt 9.17.4 om utskrifter). För att säkerställa spårbarhet i hantering av elektroniska handlingar som innehåller hemliga eller utrikesklassificerade uppgifter kan föreskriften även medföra att ett IT-system ska innehålla en central funktion för utläsning av filer ur IT-systemet och att utläsning på klientdatorer inte ska vara möjlig (se även avsnitt 12.4 om hantering av lagringsmedier i IT-system).

Åtgärder som ska vidtas för överkorsning av sekretessmarkering (avsnitt 9.5.6 och 9.5.7) och ändring eller överkorsning av informationssäkerhetsklass (avsnitt 9.6.1 och 9.6.2) på pappershandlingar kan i IT-system anpassas efter vad som är möjligt i IT-systemet. Om det ur en säkerhetslogg i ett IT-system går att utläsa hur en behörig användare har tagit del av och hanterat en hemlig handling får föreskrifterna i 2 kap. 4-5 §§

Försvarsmaktens föreskrifter om säkerhetsskydd anses vara uppfyllda vad avser:

- datum för beslut och vem som har fattat beslutet,
- krav på anteckning i register eller liggare i 2 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd och
- krav på kvittering i 2 kap. 11 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Samråd före hävande av sekretessmarkering för en kvalificerat hemlig handling[293] antecknas normalt i anteckningsfält eller motsvarande i IT-systemet eller i en särskild handling till vilken hänvisning ska göras. Det är även betydelsefullt att det ur säkerhetsloggen går att utläsa om en användare har kopierat, vidarebefordrat eller gjort utdrag ur handlingen. Detta kan utgöra sådana rutiner som ska beslutas av varje myndighet enligt 2 kap. 9 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd.

Om en hemlig uppgift i ett IT-system inte ges det säkerhetsskydd som beskrivits ovan uppfylls inte 7 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd. Ett sådant IT-system har således inte en tillräcklig informationssäkerhet för behandling av hemliga uppgifter.

Föreskriften gäller i Försvarsmakten även för ett IT-system som är avsett för behandling av utrikesklassificerade uppgifter.[294] Någon motsvarande föreskrift för sekretessklassificerade uppgifter finns inte i Försvarsmakten.

13.4 Tillträdesbegränsning kring ett IT-system

Tillträdesbegränsning har en avgörande betydelse för informationssäkerheten i ett IT-system. En person som har fysisk åtkomst till utrustning som ingår i ett IT-system kan påverka IT-systemet för att kringgå de åtgärder som ska skydda de behandlade uppgifterna eller som ska skydda IT-systemets funktion.

MUST har beslutat ett direktiv om tillträdesbegränsning i utrymmen för IT- och telekommunikation [referens 26]. Direktivet innehåller tolkning av författningskrav och ger vägledning för separering, sektionering, tvåhandsfattning och personell bevakning i sådana utrymmen. Tillträdesbegränsning beskrivs i kapitel 5 i H SÄK Skydd.

293 2 kap. 4 § andra stycket Försvarsmaktens föreskrifter om säkerhetsskydd.
294 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

13.4.1 Hemliga uppgifter

Utrymmen som innehåller växlar, korskopplingar och servrar samt datorhallar skall uppfylla de krav som gäller för skyddsnivå 2, 3 eller 4. I bilaga till dessa föreskrifter anges de krav som gäller för respektive skyddsnivå.

3 kap. 9 § Försvarsmaktens föreskrifter om säkerhetsskydd

Med växlar avses t.ex. telefonväxlar, radioväxlar, routrar, switchar, hubbar och radioaccesspunkter.

Funktionen hos tele- och dataväxlar, korskopplingar, dataservrar och motsvarande tekniska installationer som behandlar hemliga uppgifter är av sådan betydelse för myndigheternas verksamhet att de måste ges ett fysiskt skydd mot inbrott, stöld, skadegörelse och sabotage.

Om det i sådana utrymmen som anges i 9 § i detta kapitel behandlas uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/RESTRICTED skall utrymmena uppfylla de krav som gäller för skyddsnivå 2.

Om det i sådana utrymmen behandlas uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL eller HEMLIG/SECRET skall utrymmena uppfylla de krav som gäller för skyddsnivå 3.

Om det i sådana utrymmen behandlas uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/TOP SECRET skall utrymmena uppfylla de krav som gäller för skyddsnivå 4.

3 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd

Vilken skyddsnivå som ska väljas beror på vilken informationssäkerhetsklass som de hemliga uppgifterna är placerade i.

Utrymmen som anges i 9 § i detta kapitel skall vara försedda med system för inpasseringskontroll.

3 kap. 11 § Försvarsmaktens föreskrifter om säkerhetsskydd

I syfte att ha kontroll över tillträde till, och därmed även verksamhet, utrymmen och lokaler som innehåller tele- och dataväxlar, korskopplingar, dataservrar och motsvarande tekniska installationer ska dessa alltid vara försedda med system för inpasse-

ringskontroll, d.v.s. med ett passagekontrollsystem som medger loggning av tillträde. Passagekontrollsystemet monteras i anslutning till den eller de dörrar som leder in till utrymmena eller lokalerna. Loggning bör göras även vid utpassering.

> *Varje myndighet får fatta beslut som avviker från föreskrifterna i 10 § i detta kapitel under förutsättning att motsvarande säkerhetsskyddsnivå kan upprätthållas. Ett sådant beslut skall dokumenteras.*
>
> 3 kap. 12 § Försvarsmaktens föreskrifter om säkerhetsskydd

Varje myndighet får, med hänsyn till de lokala förutsättningarna, de aktuella utrymmenas eller lokalernas belägenhet och utförande, möjligheter att larma eller på annat sätt övervaka utrymmenas och lokalernas skalskydd, möjligheter att med insatsstyrka kunna ingripa innan intrång skett i utrymmena eller lokalerna m.m. fatta beslut som avviker från föreskrifterna i 3 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd. Detta undantag får bara fattas om beslutet innebär att motsvarande säkerhetsskyddsnivå kan upprätthållas.

Exempel på ett sådant beslut kan vara att i utrymmen och lokaler som bara uppfyller skyddsnivå 3, i tele- och dataväxlar, korskopplingar, dataservrar och motsvarande tekniska installationer hantera eller behandla uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/TOP SECRET, trots att krav på skyddsnivå 4 föreligger enligt 3 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Ett sådant beslut kan fattas om utrymmets skalskydd (golv, väggar, tak, dörr) förses med seismiska detektorer och en insatsstyrka kan ingripa, på plats, innan intrång i utrymmet eller lokalen skett, d.v.s. i regel inom 10 min. Det är däremot, i regel, inte möjligt att fatta beslut om verksamhet som enligt 3 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd ska bedrivas i ett utrymme eller i en lokal i skyddsnivå 3, får ske i ett skalskyddslarmat utrymme eller lokal i skyddsnivå 2 och att insats ska kunna ske innan intrång i utrymmet eller lokalen skett. Detta med anledning av att skyddsnivå 2 motstår angrepp i högst 5 minuter och det är mycket sällan som det går att garantera att en insatsstyrka kan vara på plats inom denna tid och att intrångsförsök hinner avvärjas.

13.4.2 Utrikesklassificerade uppgifter

Utrymmen som innehåller växlar, korskopplingar och servrar samt datorhallar där utrikesklassificerade uppgifter behandlas ska i Försvarsmakten ges motsvarande skydd som för hemliga uppgifter.[295]

295 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

13.4.3 Sekretessklassificerade uppgifter

Utrymmen som innehåller växlar, korskopplingar och servrar samt datorhallar, i vilka det behandlas betydande mängder sekretessklassificerade uppgifter, ska uppfylla de krav som gäller för skyddsnivå 2 vid behandling av sekretessklassificerade uppgifter enligt bilaga 1 till Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd. Sådana utrymmen eller datorhallar ska vara försedda med system för inpasseringskontroll.

3 kap. 11 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

Med *växlar* avses t.ex. telefonväxlar, radioväxlar, routrar, switchar och hubbar.

Av föreskriften framgår att utrymmen och datorhallar där det behandlas betydande mängder sekretessklassificerade uppgifter ska uppfylla krav för skyddsnivå 2. Föreskriften gäller således inte sådana utrymmen och datorhallar där det endast behandlas betydande mängder information som inte är sekretessbelagd (t.ex. Försvarsmaktens webbplats).

De lokaler (t.ex. tjänsterum, utbildningssalar, konferensrum och containrar) där en användare normalt använder ett IT-system i (t.ex. där det finns nätverksuttag) är inte sådana utrymmen som föreskriften anger. Sådana utrymmen behöver därför inte uppfylla krav på skyddsnivå 2, det kan dock finnas andra krav på sådana utrymmen.

Föreskriften tar sikte på att ge ett skydd för de sekretessklassificerade uppgifterna så att de inte röjs. En positiv bieffekt av skyddet är att utrymmena och datorhallarna ges ett fysiskt skydd mot oönskade händelser som även kan påverka tillgängligheten till informationen (t.ex. stöld, skadegörelse, sabotage eller manipulation).

I syfte att ha kontroll över tillträde till utrymmen som innehåller växlar, korskopplingar och servrar samt datorhallar ska dessa vara försedda med system för inpasseringskontroll, t.ex. ett passagekontrollsystem som medger registrering av tillträde. Passagekontrollsystemet monteras i anslutning till den eller de dörrar som leder in till utrymmena eller datorhallarna. Ett system för inpasseringskontroll kan utgöras av teknisk utrustning eller genom bevakning av personal.

13.5 Olika miljöer för ett IT-system

Ett IT-system kan finnas i flera olika miljöer, t.ex. miljöer för utveckling, test, prov- och försök, förvaltning samt drift. Skyddet i och kring en sådan miljö ska vara anpassad för de uppgifter som respektive miljö är avsedda att behandla. Om en utvecklings-

miljö är avsedd för behandling av hemliga uppgifter ska således utvecklingsmiljön ha ett säkerhetsskydd på samma sätt som en motsvarande driftmiljö som är avsedda för hemliga uppgifter ska ha.

Vid utveckling av ett IT-system som är avsett för behandling av hemliga uppgifter kan utveckling eller test ibland äga rum i en miljö som inte är avsett för hemliga uppgifter. Det är först när IT-systemet används i en driftmiljö som de hemliga uppgifterna kommer att behandlas. Om utvecklings- eller testmiljön ges ett lägre skydd än driftmiljön är det lättare för en aktör att genomföra intrång, t.ex. i syfte att kartlägga eller påverka IT-systemet. Vilket skydd en utvecklings-, test- och andra miljöer behöver måste därför uppmärksammas i de analyser som ska föregå utvecklingen av ett IT-system (avsnitt 14.1).

13.6 Dokumentation över skyddet

Varje myndighet skall dokumentera det säkerhetsskydd som finns i fråga om ett IT-system, från dess utveckling till dess avveckling. Dokumentationen skall hållas aktuell.

7 kap. 9 § Försvarsmaktens föreskrifter om säkerhetsskydd

Varje organisationsenhet ska se till att skyddet i och kring ett IT-system som inte är avsett för behandling av hemliga uppgifter är tillfredsställande. Organisationsenheten ska dokumentera det skydd som finns i fråga om IT-systemet. Dokumentationen ska hållas aktuell.

4 kap. 4 § Försvarsmaktens interna bestämmelser om IT-säkerhet

För att ett IT-systems skydd ska kunna upprätthållas under systemets livslängd är det nödvändigt att kontinuerligt dokumentera det skydd som gäller för IT-systemet. Av 1 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet följer att skyddet ska vara tillfredsställande i fråga om IT-systemet från dess utveckling till dess avveckling. Motsvarande föreskrift i fråga om IT-system som är avsedda för hemliga uppgifter finns i 7 kap. 9 § Försvarsmaktens föreskrifter om säkerhetsskydd.

Att dokumentationen ska hållas aktuell innebär att ett dokument ska ändras om det förhållande som ett dokument avser förändras. Ett exempel är de förändringar som en IT-säkerhetsspecifikation (avsnitt 14.5) genomgår inför utveckling av ett IT-system till dess att IT-systemet har avvecklats. Ett annat exempel är om ett IT-system ändras så att ritningar över IT-systemet eller elektroniska kommunikationsnät behöver ändras (avsnitt 17.3).

13.7 IT-system som inte är avsedda för hemliga eller utrikesklassificerade uppgifter

Varje organisationsenhet ska av säkerhetsskäl avstå från ett IT-system som inte är avsett för behandling av hemliga uppgifter eller begränsa dess innehåll, om erforderligt skydd inte kan uppnås eller upprätthållas. Med erforderligt skydd avses att uppgifter inte görs tillgängliga eller röjs för obehöriga personer, samt att uppgifterna är riktiga och spårbara samt tillgängliga för behöriga användare.

4 kap. 5 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Föreskriften innebär inte att en organisationsenhet kan vägra att ta emot ett IT-system som har blivit centralt ackrediterat. När den lokala ackrediteringen ska göras bör systemägaren endast ta fasta på de lokala förhållandenas påverkan på IT-systemet. Detta innebär även att systemägaren ska beakta eventuella villkor för lokal driftsättning som produktägaren har ställt upp.

Om det vid den lokala ackrediteringen uppmärksammas att IT-systemet är behäftat med brister – alltså förhållanden som produktägaren borde ha uppmärksammat och dokumenterat – måste organisationsenheten dokumentera dessa iakttagelser och anmäla förhållandet till produktägaren. Om inte annat meddelas av produktägaren, eller en överordnad enhet, bör IT-systemet kunna tas i drift vid organisationsenheten i enlighet med vad som anges i den centrala ackrediteringen. Detta under förutsättning att IT-systemet, i förekommande fall, har ackrediterats lokalt (avsnitt 19.4).

13.8 Utrustning som innehåller fast monterade lagringsmedier

En utrustning (t.ex. en bärbar dator) som innehåller ett *fast monterat lagringsmedium* som är avsett att innehålla eller som innehåller hemliga eller utrikesklassificerade uppgifter ska skyddas på ett sätt som motsvarar vad som gäller för de uppgifter som finns lagrade på lagringsmediet, t.ex. i fråga om registrering, förvaring och inventering av utrustningen.

13.9 Enanvändarsystem

Ett enanvändarsystem är ett IT-system som *administreras och används av endast en person*. Ett sådant IT-system får inte:

- vara anslutet mot något elektroniskt kommunikationsnät eller
- använda lagringsmedier för informationsutbyte med andra IT-system för att få kallas enanvändarsystem.

Ett enanvändarsystem som är avsett för behandling av hemliga eller utrikesklassificerade uppgifter ska ackrediteras innan det tas i drift (kapitel 19).[296] [297] Behov, utveckling, användning och avveckling m.m. i ett enanvändarsystems livscykel ska föregås av beslut om auktorisation.[298]

I Försvarsmaktens föreskrifter om säkerhetsskydd och Försvarsmaktens interna bestämmelser om IT-säkerhet finns många föreskrifter som inte gäller för ett enanvändarsystem. I detta avsnitt finns råd som riktas till en användare och en administratör av ett enanvändarsystem.

- Ett enanvändarsystem får installeras och konfigureras av driftpersonal, d.v.s. en annan person än användaren av IT-systemet.
- Alla nätverkstjänster måste stängas av och eventuell inbyggd brandvägg bör konfigureras till att inte tillåta inkommande eller utgående kommunikation.
- Då installationen är klar bör driftpersonalen lämna över alla eventuella lösenord och koder till enanvändarsystemet till användaren. Användaren bör byta dessa innan han eller hon börjar använda IT-systemet och förvara dessa i en förslutningspåse på en plats så att obehöriga inte kan komma åt dem. Driftpersonal bör behålla lösenord och koder till Administratörskontot på enanvändarsystemet under förutsättning att användaren kan förvara systemet så att driftspersonal inte har tillgång till det utan användarens närvaro.
- Om användaren, efter att han eller hon har börjat använda IT-systemet för behandling av hemliga eller utrikesklassificerade uppgifter, behöver hjälp av driftpersonal får användaren inte lämna datorn ifrån sig. Driftpersonalens arbete med IT-systemet bör övervakas av användaren.
- Användaren måste själv kunna göra säkerhetsuppdateringar av programvaror som ingår i IT-systemet, t.ex. operativsystem, applikationsprogramvaror och virusdefinitioner. En driftorganisation får bistå med programpaket så att användaren själv kan genomföra uppdateringarna.
- Användaren ansvarar själv för att genomföra säkerhetskopiering av de uppgifter som behandlas i enanvändarsystemet.

296 12 kap. 1 § andra stycket Försvarsmaktens interna bestämmelser om IT-säkerhet.
297 1 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
298 6 § Försvarsmaktens interna bestämmelser om IT-verksamhet.

- Det är lämpligt att använda sig av säkerhetsfunktionen för behörighetskontroll även i ett enanvändarsystem. Normalt behöver man t.ex. inte ha lika omfattande behörigheter då man arbetar i ett enanvändarsystem som man har då man administrerar systemet. Därför kan det vara lämpligt att använda två konton i ett enanvändarsystem, ett administratörskonto och ett användarkonto. Vid normalt arbete använder användaren då det vanliga användarkontot. Skulle datorn smittas av skadlig kod är sannolikheten större att skadan blir mer omfattande om man är inloggad som administratör vid smittotillfället, p.g.a. de utökade behörigheter en administratör har i systemet jämfört med en vanlig användare. En annan anledning att använda säkerhetsfunktionen för behörighetskontroll är att den kan hjälpa till att skydda mot att en obehörig person ger sig tillfällig tillgång till IT-systemet, t.ex. om personen passerar förbi systemet och det inte är övervakat av användaren.
- Man får ha flera konton på ett enanvändarsystem om alla konton används av samma användare.
- Användaren är ansvarig för alla uppgifter som behandlas i IT-systemet och alla händelser i systemet.
- Ett enanvändarsystem som innehåller ett lagringsmedium som avses innehålla eller som innehåller hemliga eller utrikesklassificerade uppgifter ska förvaras i ett förvaringsutrymme som uppfyller de krav som gäller för den informationssäkerhetsklass som lagringsmediet har placerats i (se avsnitt 12.2.10 om förvaring av lagringsmedier).
- Innan ett enanvändarsystem återlämnas till driftorganisationen bör alla ingående lagringsmedier raderas med raderingsverktyg som är godkänt för den informationssäkerhetsklass som ett lagringsmedium är placerat i. Raderingen bör göras av användaren eller av driftpersonal under användarens övervakning.
- Ett enanvändarsystem ska vara försett med en godkänd säkerhetsfunktion för skydd mot skadlig kod (avsnitt 18.4).[299]
- Ett enanvändarsystem som ska användas för behandling av hemliga eller utrikesklassificerade uppgifter som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre ska vara försett med en godkänd säkerhetsfunktion för skydd mot röjande signaler (avsnitt 18.5).[300]
- Ett lagringsmedium i ett enanvändarsystem ska registreras, märkas, inventeras och återlämnas på samma sätt som andra lagringsmedier (avsnitt 12).[301]

Vilka regler som gäller i det enskilda fallet bör framgå av ett enanvändarsystems IT-säkerhetsinstruktion (avsnitt 14.8).

---

299 11 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

300 7 kap. 13 § Försvarsmaktens föreskrifter om säkerhetsskydd och 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

301 7 kap. 3 § Försvarsmaktens föreskrifter om säkerhetsskydd, 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar och 3 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

13.10 Märkning av informationsklassificering i ett IT-system

En märkning utgör metadata till den behandlade uppgiften i IT-systemet och kan t.ex. bestå av en kodning som ingår i e-posthuvudet för en e-post eller beskrivande fält för en post i en databas. En sådan märkning avser alltså inte märkningar på en elektronisk handling som användaren har ritat (t.ex. en sekretessmarkering i en Powerpoint-fil).

I IT-system behandlas normalt olika slag av uppgifter som:

- kan omfattas av olika sekretessbestämmelser enligt OSL,
- kan tillhöra olika sekretesskategorier (kvalificerat hemlig, hemlig, utrikesklassificerad och sekretessklassificerad) och
- i vissa fall har placerats i en informationssäkerhetsklass eller
- inte omfattas av någon sekretess enligt OSL.

Sekretessbestämmelser enligt OSL avgör även i vissa fall vilka som kan få ta del av uppgifterna, t.ex. personal vid en utländsk myndighet (avsnitt 7.7). I internationella samarbeten används s.k. caveat för att begränsa delgivning eller användning av handlingar (avsnitt 7.8). I takt med att informationsutbyte mellan IT-system blir vanligare ökar behovet av att IT-systemen tekniskt kan märka uppgifter med avseende på de behandlade uppgifternas informationsklassificering m.m. Syftet är att uppgifterna inte ska behandlas i strid med föreskrifter om skydd av uppgifterna eller i strid med överenskommelser med en annan stat eller mellanfolklig organisation.

Märkning av de behandlade uppgifternas informationsklassificering underlättar en automatisk filtrering av uppgifter som ingår i ett informationsflöde mellan IT-system. En sådan filtrering kan då användas i säkerhetsfunktionen för intrångsskydd (avsnitt 18.7). Märkningen kan även användas av andra säkerhetsfunktioner, t.ex. i säkerhetsfunktionen för behörighetskontroll (avsnitt 18.3) för att verifiera att en användare har beslutats vara behörig att ta del av uppgifter som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET (avsnitt 7.3) eller för att säkerställa andra former av behörigheter enligt kapitel 7.

Märkning av de behandlade uppgifternas informationsklassificering kan även användas i ett IT-systems användargränssnitt för att t.ex. i en rapportgenerator skapa de sekretessmarkeringar och andra märkningar som en elektronisk handling ska innehålla (avsnitt 9.5.1 och 9.6). Märkningen bör även kunna användas i sökverktyg eller i register för att visa de lagrade uppgifternas informationsklassificering.

I MUST krav på godkända säkerhetsfunktioner (KSF 3.0) [referens 44] finns flera krav som rör märkning av information i ett IT-system. Där finns bl.a. krav på att informa-

tion som passerar in till ett IT-system ska märkas och att märkningen ska användas vid kontroll av information som passerar ut från ett IT-system. Utformning av märkning av informationsklassificering och andra informationssäkerhetsegenskaper måste därför analyseras i en säkerhetsmålsättning (avsnitt 14.1).

14 Analyser, planer och instruktioner för IT-säkerhet

Ett IT-system som ska kunna användas som ett stöd i verksamheten måste åtnjuta ett tillräckligt skydd. IT-systemet måste också kunna skydda de uppgifter som verksamheten behandlar. Båda dessa skyddsaspekter måste beaktas så att:

- uppgifter inte görs tillgängliga eller avslöjas för obehöriga,
- uppgifter avsiktligt eller oavsiktligt förändras,
- uppgifter är tillgängliga i förväntad omfattning, samt
- framförallt säkerhetspåverkande händelser entydigt kan härledas till identifierade användare.

För att komma fram till vilka säkerhetskrav som gäller för IT-säkerheten för ett IT-system behöver flera analyser genomföras.

I en *säkerhetsmålsättning* för ett IT-system dokumenteras analyser över vilket skydd IT-systemet kräver och vilka åtgärder som måste vidtas för att skyddet ska få avsedd effekt. En säkerhetsmålsättning för ett IT-system i Försvarsmakten innehåller därför normalt:

- verksamhetsanalys,
- regelverksanalys,
- säkerhetsanalys (avseende hot, risker och sårbarheter), samt
- IT-säkerhetsspecifikation (ITSS).

Även andra analyser kan förekomma i en säkerhetsmålsättning om det behövs för säkerhetsmålsättningens syfte.

En säkerhetsmålsättning används under ett IT-systems livscykel som ett samlat kravdokument för IT-säkerhet. Fokus i en säkerhetsmålsättning ligger på *vilka åtgärder som måste vidtas för att skyddet ska få avsedd effekt.* En säkerhetsmålsättning används bl.a. i ackrediteringsarbetet (kapitel 19) genom att granskningen utgår från målsättningen för att kunna bedöma om de framtagna skyddsåtgärderna tillgodoser de uppställda förväntningarna. Utifrån detta kan slutsatser dras om säkerheten i och kring IT-systemet är godtagbar, eller inte. En säkerhetsmålsättning ska även kunna användas som grund för en organisationsenhets IT-säkerhetsplan samt kontinuitetsplan och IT-säkerhetsinstruktion som hör till IT-systemet. Säkerhetsmålsättning beskrivs i avsnitt 14.1.

En *verksamhetsanalys* beskriver i IT-säkerhetssammanhang den verksamhet som ett IT-system är tänkt att stödja, vilka slag av uppgifter som IT-systemet är avsett att behandla samt verksamhetens krav på skydd, t.ex. i fråga om tillgänglighet. En verksamhetsanalys utgör en utgångspunkt för regelverksanalys och säkerhetsanalys. Verksamhetsanalys beskrivs i avsnitt 14.2.

En *regelverksanalys* syftar till att beskriva vilka lagar, förordningar, föreskrifter, bestämmelser och andra regler som är aktuella för ett IT-system och för de uppgifter som avses behandlas i IT-systemet. Regelverksanalys beskrivs i avsnitt 14.3.

I en *säkerhetsanalys* som hör till ett IT-system identifieras och prioriteras först de skyddsvärda tillgångarna därefter bedöms säkerhetshot, sårbarheter och risker. Identifierade risker prioriteras och beslut om hur riskerna ska hanteras fattas (riskhanteringsbeslut). Säkerhetsanalyser beskrivs utförligt i H SÄK Grunder. IT-säkerhetsspecifika överväganden beskrivs i avsnitt 14.4 i denna handbok.

En *IT-säkerhetsspecifikation* (ITSS) för ett IT-system specificerar vilka IT-säkerhetsförmågor systemet ska ha, och på vilket sätt och i vilken miljö systemet ska användas för att systemet ska anses vara tillräckligt säkert samt hur systemets säkerhetsfunktioner och driftmiljö samverkar för att säkerställa dessa säkerhetsegenskaper. En IT-säkerhetsspecifikation ska innehålla alla säkerhetskrav som ställs på ett IT-system, både *krav på säkerhetsfunktioner* samt *tillkommande säkerhetskrav* som är ett resultat av verksamhets-, regelverks- och säkerhetsanalyser. Bild 14:1 visar förhållanden mellan analyser och säkerhetskrav i en säkerhetsmålsättning.

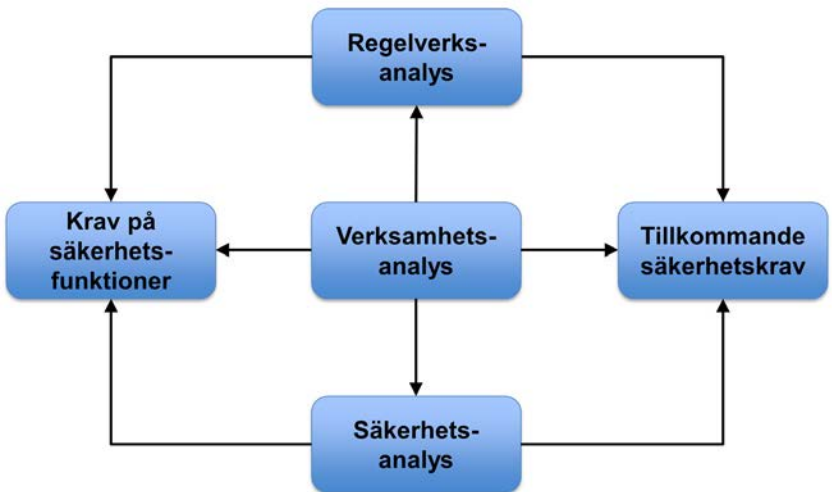


Bild 14:1 - Schematisk bild över förhållanden mellan analyser och säkerhetskrav i en säkerhetsmålsättning.

Beroende på hur omfattande och komplext ett IT-system är, kan det vara nödvändigt att genomföra och dokumentera verksamhets-, regelverks- och säkerhetsanalyser i flera steg. I många fall är dock IT-systemen och den verksamhet som de ska stödja så pass överblickbara att de olika analyserna kan genomföras och dokumenteras var för sig i ett steg. Den ovan beskrivna ordning av analyserna är den mest naturliga. I vissa enstaka fall kan det dock vara påkallat att låta säkerhetsarbetet följa en annan gång. Huvudsaken är att spårbarheten mellan de olika delresultaten i sådana fall beskrivs så att det går att följa resonemangen och slutligen bedöma om ett IT-system kan ackrediteras eller inte.

Försvarsmaktens organisationsenheter ska planera för att kunna hantera avbrott och störningar i sina IT-system.[302] Tidigare har begreppet avbrottsplanering ofta använts i Försvarsmakten som benämning på dessa planer. *Kontinuitetsplanering* beskriver på ett bättre sätt vad planeringen syftar till, nämligen att verksamheten ska kunna fortgå vid funktionsbortfall i ett IT-system. En framgångsrik kontinuitetsplanering är beroende av bl.a.

- väldefinierade IT-system med tillhörande ansvarsområden,
- delaktighet från berörda produkt-, system- och driftägare,
- testning av planeringen, samt
- återkoppling av testresultaten.

Kontinuitetsplan beskrivs i avsnitt 14.6

IT-säkerhetsplanering ska användas för att på ett spårbart sätt hantera fel och brister i och kring hanteringen av IT-system. Chefen för en organisationsenhet kan på så sätt på ett strukturerat sätt tilldela uppgifter och resurser till IT-säkerhetspersonalen och få återkoppling när felen och bristerna är åtgärdade. IT-säkerhetsplan beskrivs i avsnitt 14.7.

Inget IT-system är det andra likt. Därför är det lämpligt att det tas fram systemspecifika *IT-säkerhetsinstruktioner* som borgar för att ett IT-system kan hanteras på ett så säkert sätt som möjligt. IT-säkerhetsinstruktion beskrivs i avsnitt 14.8.

I de följande avsnitten beskrivs de olika analyserna, kravformuleringarna, planerna och instruktionerna och även exempel på vad de bör innehålla.

302 1 kap. 9 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

14.1 Säkerhetsmålsättning

Varje myndighet som överväger att införa eller använda ett IT-system som skall användas av flera personer skall noga analysera vilket säkerhetsskydd systemet kräver och vilka åtgärder som måste vidtas för att säkerhetsskyddet skall få avsedd effekt. En sådan analys skall även göras innan en myndighet upplåter ett IT-system till en annan myndighet, ett annat land eller en mellanfolklig organisation.

Analyser som avses i första stycket skall dokumenteras.

7 kap. 7 § Försvarsmaktens föreskrifter om säkerhetsskydd

Föreskriften gäller IT-system som är avsett för behandling av hemliga uppgifter och som ska användas av flera personer. Ett IT-system som ska användas av flera personer kan t.ex. vara ett elektroniskt kommunikationsnät till vilket anställdas datorer ansluts för åtkomst till gemensamma resurser såsom filservrar m.m. De datorer som är avsedda att anslutas till det elektroniska kommunikationsnätet ingår i det IT-system för vilket analysen enligt föreskriften ska genomföras. Ett annat exempel då föreskriften gäller är när ett lagringsmedium används för informationsutbyte med andra IT-system. Däremot gäller inte föreskriften för en fristående dator som inte är avsedd att användas för kommunikation med andra IT-system och inte heller användas av någon annan än den ursprungliga användaren (se avsnitt 13.9 om enanvändarsystem).

Med hänsyn till att det allt oftare förekommer att myndigheterna upplåter IT-system till andra myndigheter, andra länder eller mellanfolkliga organisationer ska nämnda analys även genomförs vid sådant upplåtande. Det är således viktigt att myndigheterna framställer sina eventuella säkerhetskrav för upplåtandet. För att få fram vilka säkerhetskrav som bör ställas måste t.ex. en säkerhetsmålsättning tas fram och dokumenteras för det IT-system som ska upplåtas.

Analyser över vilket säkerhetsskydd ett IT-system, som ska användas av flera personer, kräver och vilka krav som ska ställas på systemet ska dokumenteras av en myndighet. Analyserna bör samlas i ett dokument för varje IT-system. Det står en myndighet fritt hur ett sådant dokument ska benämns eller hur dess innehåll ska struktureras.

Utöver vad som följer av föreskrifterna om analys i 7 kap. 7 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd ska varje organisationsenhet som överväger att införa eller använda ett annat IT-system noga analysera vilket skydd ett sådant system kräver och vilka åtgärder som måste vidtas för att skyddet ska få avsedd effekt. Detsamma gäller innan en organisationsenhet upplåter ett sådant IT-system till en annan myndighet, ett annat land eller en mellanfolklig organisation.

4 kap. 1 § första stycket Försvarsmaktens interna bestämmelser om IT-säkerhet

I Försvarsmakten ska analys av vilket skydd som ett IT-system kräver och vilka åtgärder som måste vidtas för att skyddet ska få avsedd effekt genomföras för alla IT-system oavsett vilka uppgifter som systemet är avsett att behandla. En analys ska i Försvarsmakten således finnas för IT-system som är avsedda för behandling av hemliga, utrikesklassificerade eller sekretessklassificerade uppgifter eller uppgifter som inte omfattas av sekretess enligt OSL. Föreskriften innebär vidare att sådana analyser även ska genomföras för IT-system som endast är avsedda att användas av en person, s.k. enanvändarsystem (avsnitt 13.9).

Analyser som avses i 1 och 2 §§ i detta kapitel ska dokumenteras i säkerhetsmålsättningar.

4 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet

I Försvarsmakten benämns de samlade dokumenten som innehåller sådana analyser och krav för en *säkerhetsmålsättning*.[303] För att underlätta hanteringen får de olika delarna i en säkerhetsmålsättning utgöras av separata handlingar och behöver inte ingå som bilagor i en och samma handling. Innehållet i en säkerhetsmålsättning bör inte återupprepas i de analyser och kravsammanställningar som utgör säkerhetsmålsättningen.

303 4 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

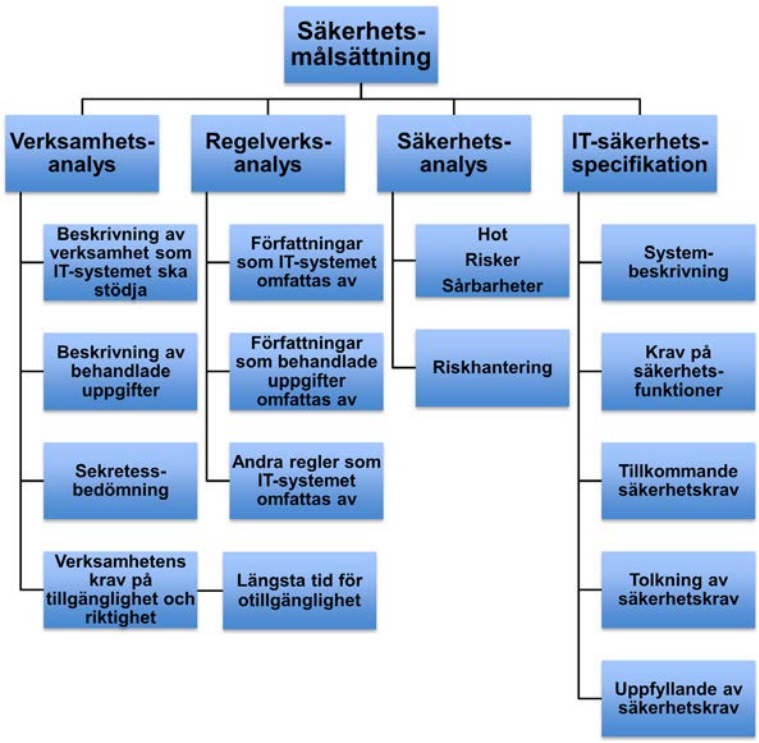


Bild 14:2 - Schematisk bild på innehållet i en säkerhetsmålsättning.

En säkerhetsmålsättning används under ett IT-systems livscykel som ett samlat kravdokument för IT-säkerhet (se avsnitt 0 för vad som avses med IT-säkerhet). Fokus i en säkerhetsmålsättning ligger på *vilka åtgärder som måste vidtas för att skyddet ska få avsedd effekt.* I IT-säkerhetspecifikationen formuleras *säkerhetskrav* för åtgärderna som kan vara olika under IT-systemets livscykel. Bild 14:2 visar schematisk innehållet i en säkerhetsmålsättning. En säkerhetsmålsättning får även innehålla andra analyser om det behövs för att uppfylla syftet med en säkerhetsmålsättning.

Då en säkerhetsmålsättning ska användas under ett IT-systems livscykel kan dess innehåll behöva ändras under livscykeln. En säkerhetsmålsättning består således inte av ett eller flera statiska dokument. Detta gäller i synnerhet inför och under utveckling av ett IT-system (se även avsnitt 13.6 om dokumentation). Omfattningen av dokumentation i en säkerhetsmålsättning (bild 14:2) kan naturligtvis variera beroende på vilket IT-system som avses.

Inom ramen för Försvarsmaktens IT-styrmodell (avsnitt 2.3) och auktorisationsprocess ges de inriktningar som avser omfattning och innehåll på säkerhetsmålsättningen med dess ingående delar.

Om de analyser som ingår i en säkerhetsmålsättning ger vid handen att det finns föreskrifter som inte bedöms kunna följas måste detta hanteras, i god tid, genom undantagshantering (se H SÄK Grunder). Särskilt viktigt är att då beskriva:

- Vilka risker som inte möts av säkerhetsfunktioner.
- Vilka kvarvarande sårbarheter som bedöms finnas.
- Vilka författningskrav som inte bedöms uppfyllas.

Om det för ett IT-system finns beslut om undantag från Försvarsmaktens föreskrifter eller interna bestämmelser är det lämpligt att säkerhetsmålsättningen redovisar detta.

14.1.1 Säkerhetsmålsättning vid materielanskaffning

Vid anskaffning av materiel som utgör eller innehåller IT-system måste kraven på IT-säkerhet uppmärksammas. Med olika målsättningsarbeten kan det finnas en risk att krav på IT-säkerhet inte uppmärksammas på samma sätt som de funktionella kraven i t.ex. TTEM. Ett målsättningsdokument som används vid materielanskaffning bör minst hänvisa till den säkerhetsmålsättning som gäller för IT-systemet. Målsättnings- och kravdokument får även återge krav i en säkerhetsmålsättning för att få en sammanhållen kravbild.

Kraven i en säkerhetsmålsättning kan behöva kopplas mot krav i TTEM (som är ägarföreträdarnas ansvar) respektive krav i kravspecifikationer som tekniskt designansvariga tar fram inför upphandling.

Tiden från att materiel anskaffas till att den avvecklas kan vara lång. Det är viktigt att under materielens livscykel uppmärksamma förändringar i krav på informationssäkerhet, t.ex. till följd av ändrade författningar.

14.2 Verksamhetsanalys

Se H SÄK Grunder för en allmän beskrivning av verksamhetsanalys. I IT-säkerhetssammanhang bör en verksamhetsanalys beskriva den verksamhet som IT-systemet är tänkt att stödja, vilka slag av uppgifter som IT-systemet är avsett att behandla samt verksamhetens krav på skydd.

Följande punkter är en vägledning för att utarbeta sådana beskrivningar.

1. Vilken verksamhet ska IT-systemet stödja?
   - Nationellt – internationellt?
   - Fred – kris – krig?
   - Kommer personal från en annan stat eller mellanfolklig organisation använda IT-systemet?

- Är IT-systemet avsett för användning utanför Försvarsmaktens objekt, lokaler och områden?
- Är IT-systemet avsett för distansarbete (avsnitt 15.3)?

2. Vem har ansvaret för den verksamhet som IT-systemet ska stödja?
3. Vem har ansvaret för IT-systemet och i vilken roll?
4. Vilka resurser finns för att skydda IT-systemets delar och informationen i dessa?
5. Vilka andra verksamheter eller organisationsenheter är beroende av den verksamhet som IT-systemet ska stödja?
   - Vilka funktioner – vilken information?
6. Vilka (andra) verksamheter eller organisationsenheter är beroende av IT-systemet?
   - Vilka funktioner – vilken information?
7. Behandlad information
   - Vilken typ av information är IT-systemet avsett att behandla?
   - Sekretessbedömning enligt avsnitt 14.2.1.
   - Finns begränsningar av vem som får behandla uppgifter i IT-systemet?
   - Finns begränsningar för personal från en annan stat eller mellanfolklig organisation att ta del av uppgifter som behandlas i IT-systemet (avsnitt 7.7)?
   - Finns begränsningar (caveat) i att delge eller använda uppgifter som avses behandlas i IT-systemet (avsnitt 7.8)?
   - Verksamhetens krav på tillgänglighet (avsnitt 14.2.2).
   - Verksamhetens krav på riktighet.
   - Verksamhetens behov av nödöppning (avsnitt 7.11).
8. Kommunikation
   - Vilket behov finns att överföra information på flyttbara lagringsmedier?
   - Vilket behov finns att överföra information genom elektroniska kommunikationsnät?
   - Övrig kommunikation till andra IT-system?

Det är lämpligt att verksamhetsanalysen genomförs före regelverksanalysen och säkerhetsanalysen för att undvika att de efterföljande analyserna får felaktiga ingångsvärden. En analys med felaktiga ingångsvärden kan medföra att uppgifterna i ett IT-system inte får det skydd som de egentligen borde ha haft. I IT-säkerhetssammanhang dokumenteras verksamhetsanalysen som en del i säkerhetsmålsättningen.

En *arkivredovisning* kan vara ett underlag för verksamhetsanalysen. Redovisningens funktion är att göra det möjligt att förstå sambanden mellan verksamhet och handlingar, överblicka handlingsbeståndet, söka och ta fram handlingar samt hantera och förvalta handlingar. Arkivredovisningen är oberoende av om handlingarna finns på

papper eller i elektronisk form i ett IT-system. Läs mer i Riksarkivets *Redovisa verksamhetsinformation - Vägledning till Riksarkivets föreskrifter om arkivredovisning*.

14.2.1 Sekretessbedömning

> *Varje myndighet som beslutar att anskaffa eller förändra ett IT-system skall, för att kunna fastställa erforderligt säkerhetsskydd för systemet, göra en sekretessbedömning av såväl de enskilda uppgifterna som den totala informationsmängden som avses hanteras i IT-systemet.*
>
> 7 kap. 8 § Försvarsmaktens föreskrifter om säkerhetsskydd

Varje myndighet, och organisationsenhet i Försvarsmakten, ska undersöka vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet.[304] [305] I IT-säkerhetssammanhang ska sekretessbedömning minst klarlägga om det finns hemliga uppgifter i ett IT-system. För att ett IT-system ska ha ett tillräckligt säkerhetsskydd är det nödvändigt att bedöma de slag av uppgifter som systemet är tänkt att behandla. Resultatet av en sådan bedömning ska ange vilka slag av uppgifter som omfattas av sekretess enligt OSL och i vilken utsträckning uppgifterna är hemliga samt i vilka informationssäkerhetsklasser som uppgifterna placeras i. I en sådan bedömning måste hänsyn tas till möjligheten att kombinera flera uppgifter (aggregation) så att *nya uppgifter* erhålls som inte hade varit möjlig att få med tillgång endast till uppgifterna var och en för sig. Se H Säk Sekrbed A om aggregation.

En sekretessbedömning ska även tjäna till att ett IT-system inte ges ett högre skydd än vad som är nödvändigt. Detta är särskilt viktigt eftersom skyddsåtgärder oftast är kostnadsdrivande.

Ett ingångsvärde för att bestämma erforderligt säkerhetsskydd för ett IT-system är om uppgifterna som avses behandlas i IT-systemet är hemliga och i vilken högsta informationssäkerhetsklass som uppgifterna, enskilt eller sammantaget, kan komma att placeras i. Om ett IT-system är avsett för hemliga uppgifter ger den högsta informationssäkerhetsklassen för uppgifterna:

- vilka säkerhetsfunktioner (avsnitt 13.2) som ska finnas i systemet och
- vilka tillkommande säkerhetskrav (avsnitt 13.3) som gäller för systemet samt
- vilken skyddsnivå som gäller för vissa utrymmen och datorhallar där IT-systemet placeras (avsnitt 13.4).

304 5 § säkerhetsskyddsförordningen.
305 1 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

Föreskriften gäller i Försvarsmakten även för ett IT-system som är avsett för behandling av utrikesklassificerade uppgifter.[306] En sekretessbedömning i Försvarsmakten ska även klarlägga om ett IT-system är avsett för behandling av sekretessklassificerade uppgifter eller uppgifter som inte omfattas av sekretess enligt OSL.[307]

I Försvarsmakten används modellen för informationsklassificering med avseende på sekretess enligt H Säk Sekrbed A. Om ett IT-system är avsett att behandla uppgifter som omfattas av sekretess enligt OSL bör en verksamhetsanalys beskriva

- sekretessbestämmelser enligt OSL,
- sekretesskategori (kvalificerat hemlig, hemlig, utrikesklassificerad eller sekretessklassificerad) samt
- eventuell placering i informationssäkerhetsklass som bedöms gälla för uppgifterna.

14.2.2 Verksamhetens krav på tillgänglighet

Det bör framgå av en verksamhetsanalys om ett IT-system är avsett för någon verksamhetskritisk information. Vilka slag av uppgifter som bedöms vara verksamhetskritiska bör då anges. En vägledning kan vara om IT-systemet är avsett för behandling av t.ex. stridsledningsdata, elektroniska fakturor, personuppgifter, patientjournaler eller underrättelser.

Det bör beskrivas i en verksamhetsanalys i vilken utsträckning som uppgifterna som avses behandlas i IT-systemet måste vara tillgängliga i en förutbestämd omfattning. Det är också lämpligt att det av verksamhetsanalysen framgår den *längsta tid som ett IT-system bedöms kunna vara ur funktion* utan att verksamheten i väsentlig omfattning störs. En sådan tid kan vara olika för olika skeden, vilket då bör beskrivas. I denna del utgör verksamhetsanalysen grund för IT-systemets kontinuitetsplan (avsnitt 14.6).

Tillgänglighet avser här inte ett IT-systems användarvänlighet eller i vilken utsträckning funktionshindrade kan använda IT-systemet.

306 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

307 1 kap. 7 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

14.3 Regelverksanalys

Tidigare kallades denna analys för *författningsanalys*. Det kan finnas krav på IT-säkerhet som inte kan sägas utgöra författningskrav men som måste uppmärksammas i kravarbetet. Sådana krav bör tas med i regelverksanalysen för att de inte ska tappas bort. Ett exempel är krav på IT-säkerhet som kommer från anslutning av ett IT-system till ett elektroniskt kommunikationsnät och som har ställts av den som svarar för nätet (avsnitt 17.2). Att sådana krav finns är anledningen till att denna analys numera kallas *regelverksanalys*.

I utvecklingen av ett IT-system är det viktigt att analysera vilka *lagar*, *förordningar*, *föreskrifter*, *bestämmelser* och andra regler som *IT-systemet* omfattas av. Lika viktigt är det att analysera motsvarande för de *uppgifter som IT-systemet* är avsett *att behandla*. En regelverksanalys syftar till att belysa detta. Verksamhetsanalysen är ett ingångsvärde för en regelverksanalys, t.ex. vad gäller resultatet av en sekretessbedömning av de uppgifter som IT-systemet är avsett att behandla.

Resultatet från regelverksanalysen dokumenteras i säkerhetsmålsättningen och används för att kunna formulera de säkerhetskrav som ställs på ett IT-system. Beskrivningen av vilka författningar som är aktuella behöver inte resultera i en uttömmande avskrift av alla tillämpliga paragrafer, det tar bara plats och tillför sällan något mervärde. Istället kan en beskrivning för t.ex. ett IT-system som är avsett för behandling av hemliga uppgifter vilka har placerats i en informationssäkerhetsklass formuleras enligt exemplet nedan.

Exempel 14:1

IT-systemet omfattas av Försvarsmaktens föreskrifter (2003:7) om säkerhetsskydd i allmänhet och de föreskrifter som styr säkerhetsskyddet för informationssäkerhetsklassen HEMLIG/CONFIDENTIAL i synnerhet.

En regelverksanalys ska således inte gå till överdrift. En säkerhetsmålsättning för ett IT-system som är avsett för behandling av hemliga uppgifter och som därmed ska ha ett säkerhetsskydd behöver t.ex. inte återge föreskrifterna i 19 kap. brottsbalken om brott mot rikets säkerhet.

I en författning förekommer ofta paragrafer som innehåller en upplysning om andra författningar (vanligen en hänvisning till föreskrifter i andra författningar) eller en definition. Sådana ska inte tas med då upplysningsparagrafer i sig inte kommer att kunna tolkas och omsättas till ett säkerhetskrav. En anledning att inte skriva av varje föreskrift i en regelverksanalys är att författningarna ändras och då blir avskrifterna inte korrekta.

Mer meningsfullt är när en föreskrift som har identifierats tolkas och omsätts till en eller flera konkreta säkerhetskrav som är formulerade så att de är *entydiga*, *kompletta* och *mätbara*. Detta gäller i synnerhet för en föreskrift som inte bedöms uppfyllas genom någon av de sju definierade säkerhetsfunktionerna (avsnitt 13.2).

För ett IT-system som är avsett för behandling av hemliga uppgifter måste regelverksanalysen särskilt uppmärksamma de *tillkommande säkerhetskrav* som följer av portalparagrafen 7 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd (avsnitt 13.3). I Försvarsmakten gäller det även för ett IT-system som är avsett för behandling av utrikesklassificerade uppgifter.[308]

Om en författning eller en enskild paragraf inte tas med i regelverksanalysen innebär det inte att författningen eller den enskilda paragrafen inte gäller för IT-systemet eller för uppgifterna som avses behandlas. Säkerhetsmålsättningen är inte en selektering av vilka föreskrifter som faktiskt kommer att gälla. Vilka författningar som faktiskt gäller styrs av författningarna, inte av vilka som har tagits med i en regelverksanalys.

Att en regelverksanalys inte återger varje enskild paragraf hindrar inte att paragraferna inför och under utveckling förs in i kravhanteringsarbetet (t.ex. återges i ett Excel-ark). Ett strukturerat kravhanteringsarbete är ofta nödvändigt för att säkerställa att olika slag av krav omhändertas i utvecklingsarbetet.

14.4 Säkerhetsanalys

> *Varje myndighet skall genomföra och dokumentera analyser avseende vilka hot, risker och sårbarheter som kan påverka myndighetens säkerhetskänsliga verksamhet och utifrån analyserna vidta lämpliga säkerhetsskyddsåtgärder.*
>
> 1 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd

Föreskriften innebär ur ett IT-säkerhetsperspektiv att en myndighet, eller en organisationsenhet i Försvarsmakten, ska genomföra säkerhetsanalyser över vilka *hot*, *risker* och *sårbarheter* som *kan finnas* eller *finns* för ett IT-system samt med analyserna som grund vidta säkerhetsskyddsåtgärder. För ett IT-system är det nödvändigt att analysera såväl *aktörsdrivna hot* som *icke aktörsdrivna hot*. Beskrivningar av hot mot IT-system finns i H SÄK IT Hot. Hur en säkerhetsanalys genomförs i Försvarsmakten beskrivs i H SÄK Grunder.

308 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Med *säkerhetskänslig verksamhet* avses verksamhet av betydelse för rikets säkerhet.[309]

I 5 § säkerhetsskyddsförordningen (1996:633) finns föreskrifter om säkerhetsanalys. Vad som där föreskrivs om sådan analys och dokumentation ska fullgöras av varje organisationsenhet.

Av 1 kap. 6 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd och 2 § i detta kapitel följer att varje organisationsenhet ska göra hot-, risk- och sårbarhetsanalyser, vilka ska ingå i en säkerhetsanalys. Med säkerhetsanalysen som grund ska en säkerhetsplan upprättas.

1 kap. 5 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel

I 5 § säkerhetsskyddsförordningen (1996:633) finns föreskrifter om säkerhetsanalys. Vad som där föreskrivs om sådan analys samt dokumentation ska fullgöras av varje organisationsenhet.

1 kap. 5 § Försvarsmaktens interna bestämmelser om IT-säkerhet

I Försvarsmakten ingår en *hot-, risk- och sårbarhetsanalys* i en *säkerhetsanalys*. I fråga om en hot-, risk- och sårbarhetsanalys för ett IT-system används i denna handbok därför benämningen *säkerhetsanalys* för *hot-, risk- och sårbarhetsanalys*. Motsvarigheten till en säkerhetsplan för ett IT-system är de säkerhetskrav som dokumenteras i en *säkerhetsmålsättning* (avsnitt 14.1).

Av 1 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd och 1 kap. 4 § denna författning följer att varje organisationsenhet ska göra hot-, risk- och sårbarhetsanalyser. Sådana analyser ska även göras i fråga om övriga IT-system.

4 kap. 1 § andra stycket Försvarsmaktens interna bestämmelser om IT-säkerhet

En säkerhetsanalys ska genomföras för alla IT-system i Försvarsmakten oavsett vilka slag av uppgifter som IT-systemet är avsett att behandla.

309 1 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd och 4 § 3 säkerhetsskyddsförordningen.

Varje garnisonschef eller den han bestämmer ska genomföra och dokumentera hot-, risk- och sårbarhetsanalyser i fråga om ett IT-system som ska användas gemensamt inom garnisonen och utifrån analyserna vidta lämpliga skyddsåtgärder.

4 kap. 2 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Rollen garnisonschef förekommer inte längre i FM ArbO. Det är produktionschefen som ska leda och samordna verksamheten mellan organisationsenheter (garnisonssamordning) inom samma kommun eller liknande samordning mellan organisationsenhter i olika kommuner.[310]

En säkerhetsanalys för IT-system som ska användas gemensamt inom en garnison genomförs inom ramen för garnisonssamordning.

I fråga om hot som kan orsaka avbrott i en verksamhet utgör en säkerhetsanalys ett underlag för kontinuitetsplanen för ett IT-system (avsnitt 14.6).

Hot som är omhändertagna av de sju säkerhetsfunktionerna (avsnitt 13.2) behöver vanligtvis inte ges någon större uppmärksamhet i en säkerhetsanalys. Det generella hotet ”virus i IT-system” ska t.ex. vara reducerat av den obligatoriska säkerhetsfunktionen för skydd mot skadlig kod. En säkerhetsanalys bör istället fokuseras på sådana hot-, risker- och sårbarheter som är *unika för det specifika IT-systemet*. Det kan t.ex. vara fråga om sårbarheter till följd av miljön vid de platser där IT-systemet ska placeras. Kända brister i skyddet i och kring ett IT-system bör därför ges större uppmärksamhet i en säkerhetsanalys. Sådana kända brister kan även avse brister i de sju säkerhetsfunktionerna.

För att kunna genomföra en säkerhetsanalys, måste en hotbild mot verksamheten och IT-systemet vara framtagen (säkerhetshotbedömning). Generellt underlag kan hämtas ur H Säk IT Hot och H Säk Hot. Behov av specifika säkerhetshotbedömningar inför en säkerhetsanalys anmäls till säkerhetskontoret vid MUST.

14.4.1 Riskhanteringsbeslut

Det finns tre förutsättningar för riskhantering där en risk accepteras. Antingen står ett riskhanteringsbeslut inte i strid med berörda författningar eller beslutas en *avvikelse* från Försvarsmaktens författningar eller så måste ett *undantag* från Försvarsmaktens författningar medges (se H SÄK Grunder).

310 9 kap. 6 § Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).

14.5 IT-säkerhetsspecifikation

En IT-säkerhetsspecifikation för ett IT-system innehåller bl.a. samtliga säkerhetskrav som gäller för systemet. Vad en IT-säkerhetsspecifikation (ITSS) ska innehålla och hur innehållet ska struktureras anges i MUST krav på godkända säkerhetsfunktioner (KSF 3.0) [referens 44].

14.6 Kontinuitetsplan

> *Varje organisationsenhet ska i en plan ange vilka åtgärder som ska vidtas vid avbrott eller störningar i IT-systemets funktion.*
>
> 1 kap. 9 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Försvarsmaktens organisationsenheter ska planera för att kunna hantera avbrott och störningar i sina IT-system. Planeringen syftar till att skydda en organisationsenhets IT-system, mot avbrott och effekter av oförutsedda och oönskade allvarliga händelser, så att verksamheten kan bedrivas fortlöpande. Sådana oönskade allvarliga händelser avser *i första hand inte krig* utan även oönskade händelser som kan inträffa under fred, t.ex. elavbrott, översvämning, brand, inbrott med stöld av datorer, fel i klimatanläggningar m.m. Synsättet att kontinuitetsplanering endast avser förberedelser för krig är fel.

Tidigare har begreppet avbrottsplanering ofta använts i Försvarsmakten som benämning på dessa planer. Kontinuitetsplanering beskriver på ett bättre sätt vad planeringen syftar till, nämligen att verksamheten ska kunna fortgå vid funktionsbortfall i ett IT-system. Viktigt för en framgångsrik kontinuitetsplanering är, förutom delaktighet från berörda parter, regelbundna tester av planeringen och återkoppling av testresultaten så att planeringen kan förbättras.

Kontinuitetsplanering bör omfatta tre huvudmoment:

- Omedelbara åtgärder vid systembortfall.
- Rutiner för fortsatt verksamhet utan IT-stöd.
- Återhämtning av verksamhet med IT-stöd.

Det är av stor vikt att gränsdragningen mellan verksamheten och IT-stödet är tydlig så att det inte uppstår luckor i kontinuitetsplaneringen eller att resurser på t.ex. systemägarsidan tas i anspråk för att lösa något som redan hanteras av driftorganisationen. Kontinuitetsplanering bör i möjligaste mån göras gemensamt mellan system- och driftägarföreträdare och ingå som en del i en SLA (engelska: Service Level

Agreement). För system som används gemensamt inom en garnison är det lämpligt att kontinuitetsplaneringen genomförs inom ramen för garnisonssamordningen.

Som utgångspunkt för kontinuitetsplaneringen är det lämpligt att säkerhetsmålsättningar och ackrediteringsunderlag som hör till ett IT-system används. Det är också viktigt att det är och har varit god ordning på utvecklingen av berört IT-system, dokumentationen samt att berörd personal har genomgått erforderlig utbildning med godkänt resultat.

Förutom att en kontinuitetsplan bör ange vem som är ansvarig för vad på system- respektive driftägarsidan bör det även bl.a. framgå:

- nyckelpersonalberoenden,
- vilken systemdokumentation som finns och var den förvaras,
- kritiska systemresurser och processer,
- vilka åtgärder som får vidtas med olika systemdelar,
- hur planeringen ska underhållas, samt
- när tester ska genomföras.

14.7 IT-säkerhetsplan

Chefen för en organisationsenhet ska i en skriftlig plan (IT-säkerhetsplan) fastställa riktlinjer för IT-säkerheten inom organisationsenheten.

1 kap. 10 § Försvarsmaktens interna bestämmelser om IT-säkerhet

IT-säkerhetsplanen bör beskriva de åtgärder som utgör grunden för skyddet av organisationsenhetens IT-system.

IT-säkerhetsplanering ska användas för att på ett spårbart sätt hantera fel och brister i och kring hanteringen av IT-system. IT-säkerhetsplaneringen låter chefen för en organisationsenhet på ett strukturerat sätt tilldela uppgifter och resurser till personalen för att förebygga och åtgärda eventuella fel och brister samt att få återkoppling när dessa är åtgärdade.

En IT-säkerhetsplan vid en organisationsenhet kan antingen vara generell för alla IT-system som förekommer vid organisationsenheten eller specifikt utformad för respektive IT-system. Planen bör bygga på:

1. ackrediteringsunderlag,
2. driftförutsättningar,
3. den lokala säkerhetsanalysen,
4. resultat från kontrollverksamhet, samt
5. IT-säkerhetsrelaterade incidenter och säkerhetsrapporter.

Med detta som bakgrund går det inte att här ge ett uttömmande exempel på vad som kan eller ska ingå i en IT-säkerhetsplan. Det kan dock konstateras att en IT-säkerhetsplan ska ta upp sådana omständigheter som måste åtgärdas av någon ansvarig inom en viss angiven tidsrymd givet vissa resurser för att skyddet för berört IT-system ska kunna sägas vara tillräckligt. Återkommande (periodiska) uppgifter kan som regel överföras till organisationsenhetens arbetsordning eller motsvarande. På så sätt renodlas IT-säkerhetsplanen och den blir lättare att hantera och följa upp.

Exempel 14:2

Om det vid en internkontroll vid en organisationsenhet har konstaterats att användarna saknar adekvat IT-säkerhetsutbildning för IT-systemet X bör det, förutom i kontrollprotokollet, föras in i IT-säkerhetsplanen vem som är ansvarig för att sådan utbildning genomförs, med vilka resurser samt när utbildningsinsatsen ska vara genomförd.

När denna brist är åtgärdad noteras detta för spårbarhetens skull i IT-säkerhetsplanen.

Om det inte har skett tidigare, ska åtgärdade punkter strykas när IT-säkerhetsplanen revideras.

14.8 IT-säkerhetsinstruktion

Inget IT-system är det andra likt. Därför är det lämpligt att det tas fram systemspecifika IT-säkerhetsinstruktioner som hanterar lokala förhållanden som påverkar säkerheten i och kring ett IT-system. Sådana instruktioner medför att Försvarsmaktens IT-system kan hanteras på ett så säkert sätt som möjligt.

En IT-säkerhetsinstruktion bör utgå från ackrediteringsunderlag och driftförutsättningarna och innehålla en förteckning över nyckelpersonal på system- och driftägarsidan samt deras uppgifter och ansvarsförhållanden. Instruktionen kan t.ex. beskriva vem som har rätt att besluta om tilldelning, borttagning eller spärrning av behörigheter i ett IT-system (avsnitt 18.3.6). Andra punkter i instruktionen kan vara vem på

driftsidan som får lägga upp användarkonton och hantera driftjournaler. Driftåtgärder då skadlig kod upptäcks (avsnitt 18.9.4) och avstängning av säkerhetslogg (avsnitt 18.4.2) är andra punkter som bör tas med.

En IT-säkerhetsinstruktion redovisar således specifika detaljbestämmelser för respektive IT-system och tas lämpligen fram i samband med lokal ackreditering.

15 Användning av IT-system

IT-system förekommer praktiskt taget i all teknisk materiel såväl i Försvarsmakten som i samhället i övrigt. Idag använder en stor del av befolkningen IT-system dagligen och det är inget undantag för Försvarsmaktens personal. Försvarsmakten förser sin personal med IT-system i form av t.ex. Försvarsmaktens arbetsplats (FM AP), fristående datorer och tjänstemobiler i form av smarta telefoner. För hantering av Försvarsmaktens IT-system så finns det ett omfattande regelverk som bl.a. ska minimera riskerna för informationsförluster.

Grundläggande för användning av ett IT-system är att IT-systemet ska vara godkänt för behandling av de uppgifter som en användare tänker behandla i IT-systemet.

15.1 Regler för användning av Försvarsmaktens IT-system

Försvarsmaktens IT-system är i första hand till för att lösa arbetsuppgifter. Det är dock tillåtet att under förutsättningar som anges nedan få använda t.ex. e-post, smarta telefoner och Internet för privata ändamål.

Sedan 2005 gäller *Beslut om regler för användning av Försvarsmaktens IT-system* [referens 6]. Beslutet gäller för all personal i Försvarsmakten som ska använda Försvarsmaktens IT-system, d.v.s. både civil och militär personal.[311]

I beslutet anges särskilt vad som ska gälla för uppdragstagare (t.ex. konsulter) som kommer att använda Försvarsmaktens IT-system.

Alla användare måste skriva på att de har tagit del av reglerna för att få använda IT-systemen, vare sig de tänker använda dem för privat bruk eller inte. Om man även vill ha möjlighet att använda IT-systemen för privata ändamål måste man dessutom lämna sitt samtycke till att Försvarsmakten får genomföra kontroller från säkerhetssynpunkt av både nätverkstrafiken och vad man lagrar i Försvarsmaktens IT-system, även vad avser dess innehåll. Ett sådant samtycke är frivilligt, men den som väljer att inte lämna sitt samtycke får då heller inte använda IT-systemen för privata ändamål, t.ex. skicka privata e-postmeddelanden, öppna bifogade filer i mottagna e-post-meddelanden eller lagra filer av privat karaktär. Den privata användningen får heller inte vara av sådan omfattning att den inkräktar på användarens tjänsteutövning.

311 Med militär personal avses detsamma som i 2 kap. 2 § förordningen med bestämmelser för Försvarsmaktens personal.

Varje organisationsenhet ska se till att alla vid enheten kvitterar att de har tagit del av beslutet samt att de bereds möjlighet till att lämna sitt samtycke enligt ovan. Dessutom ska organisationsenheten se till att kvittenserna förvaras samlade vid enheten. I samband med att en person anställs eller byter organisationsenhet är det lämpligt att reglerna gås igenom och att personen ges möjlighet att lämna samtycke. Kvittenserna kan lämpligtvis förvaras i personens personalakt. Kvittenserna får gallras om det finns en gallringsföreskrift.

Om man använder IT-systemen i strid mot beslutet kan organisationsenheten vidta åtgärder som t.ex. att en användares åtkomst till ett IT-system helt eller delvis begränsas eller att arbetsrättsliga åtgärder vidtas. En arbetsrättslig åtgärd kan t.ex. vara ett chefssamtal.

En användare får inte använda myndighetens IT-system på ett sådant sätt att det finns risk för att Försvarsmaktens anseende skulle kunna skadas eller att användningen kränker någon annan person. Försvarsmaktens anseende skulle t.ex. kunna skadas om en användare besöker pornografiska hemsidor på Internet, eftersom det då är myndighetens IP-adress som exponeras. Om en användare t.ex. lagrar pornografiskt material i myndighetens IT-system föreligger en risk för att detta material kan spridas, vilket kan innebära att användaren därmed kränker andra personer.

15.1.1 Vad användaren särskilt ska beakta

I *Beslut om regler för användning av Försvarsmaktens IT-system* [referens 6] anges vad en användare särskilt ska beakta när han eller hon använder ett IT-system:

- Meddelanden (t.ex. e-post) är normalt inte skyddade från insyn.
- E-post kan komma att uppfattas som myndighetens e-post.
- Prenumeration på nyhetsbrev m.m. kan generera skräppost (s.k. spam).
- Internetsurfande lämnar spår.
- Nätverkstrafik och dess innehåll loggas och lagras. Vad som i övrigt lagras loggas. Användaren måste dock observera att Försvarsmakten inte har någon skyldighet att se till att användarens privata filer säkerhetskopieras.
- Användning får inte stå i strid med någon föreskrift i författning, som t.ex. 4 kap. 9 c § brottsbalken (dataintrång).
- Programvaror som inte är auktoriserade får inte förekomma.[312]

312 6 § Försvarsmaktens interna bestämmelser om IT-verksamhet.

Utöver vad som framgår av beslutet måste användaren även beakta följande.

- Det ska finnas ett dokumenterat beslut på att användaren är behörig att använda ett IT-system.[313]
- Användaren ska ha fått utbildning på sitt IT-system, så att han eller hon på ett säkert sätt kan hantera systemet.[314] Utbildningen kan t.ex. omfatta:
  - hur information får föras in eller ut ur systemet,
  - hur informationen kontrolleras avseende skadlig kod,
  - hur skyddet mot röjande signaler (RÖS) i IT-system som är avsett för behandling av hemliga eller utrikesklassificerade uppgifter som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre ska vara omhändertaget samt
  - hur eventuella säkerhetsuppdateringar ska genomföras.
- Användaren ska också ha genomgått utbildning i IT-säkerhet och blivit godkänd.[315]
- Användaren ska säkerställa att inga obehöriga personer kan komma åt kod eller kort som ger behörighet till ett IT-system.[316] Användaren är personligt ansvarig för aktiviteter som sker när han eller hon är inloggad och får därför aldrig låna ut en kod eller ett kort. Aktiviteter som kan påverka säkerheten i IT-systemet registreras och kan komma att kontrolleras.[317]
- Användaren får aldrig ansluta sitt IT-system till ett annat nätverk än det är avsett för. En sådan anslutning kan innebära informationsförluster med allvarliga konsekvenser som följd.
- Vid utskrift av sekretessbelagda handlingar måste användaren säkerställa att alla sidor blev utskrivna och att inga sidor lämnas kvar i utmatningsfacket. Vid papperstrassel måste alla sidor tas omhand i skrivaren.
- Vid service eller administration av IT-system som är avsett för sekretessbelagda uppgifter ska användaren säkerställa att personal som är obehörig till uppgifterna som finns på datorn inte kan ta del av dem. Det kan innebära att användaren måste övervaka ett sådant arbete. Är det inte möjligt ska han eller hon fråga sin säkerhetschef om råd.
- Användaren bör tänka på att även sådan utrustning som ingår i ett IT-system som t.ex. en skärm eller en projektor bör placeras med hänsyn till dörrar och fönster, så att inga obehöriga kan se vad som visas.

313 7 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
314 6 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
315 6 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
316 7 kap. 2 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
317 7 kap. 11 § Försvarsmaktens föreskrifter om säkerhetsskydd och 8 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

15.1.2 Uppdragstagare

Om en uppdragstagare (t.ex. en konsult) ska ges tillgång till Försvarsmaktens IT-system ska det av avtalet mellan Försvarsmakten och uppdragstagaren (den juridiska personen) framgå att reglerna i *Beslut om regler för användning av Försvarsmaktens IT-system* [referens 6] ges motsvarande tillämplighet på uppdragstagaren.

15.1.3 Övriga användare av Försvarsmaktens IT-system

Beslut om regler för användning av Försvarsmaktens IT-system [referens 6] gäller inte för t.ex. utländska elever eller elever vid Försvarsmaktens skolor som har anställning utanför Försvarsmakten. För dessa gäller istället *Riktlinjer för de användare av Försvarsmaktens IT-system som inte omfattas av Beslut om regler för användning av Försvarsmaktens IT-system (HKV 2004-10-29 20 400:75133)* [referens 8]. Dessa riktlinjer är också översatta till engelska [referens 11]. I princip gäller samma regler för samtliga användarkategorier.

Varje organisationsenhet ska se till att användare av Försvarsmaktens IT-system som inte omfattas av *Beslut om regler för användning av Försvarsmaktens IT-system* [referens 6] tar del av *Riktlinjer för de användare av Försvarsmaktens IT-system som inte omfattas av Beslut om regler för användning av Försvarsmaktens IT-system (HKV 2004-10-29 20 400:75133)* [referens 8]. I samband med detta ska användarna även beredas möjlighet att lämna samtycke till att Försvarsmakten får genomföra kontroller från säkerhetssynpunkt av nätverkstrafik och vad som lagras i Försvarsmaktens IT-system, även vad avser innehåll, och därigenom ges möjlighet till privat användning av Försvarsmaktens IT-system. Varje organisationsenhet ska se till att lämnade samtycken förvaras samlade vid organisationsenheten.

15.1.4 Vilka begränsningar kan göras?

Försvarsmakten har givetvis rätt att begränsa tillgången till myndighetens IT-system. Inom myndigheten är det produktägaren (eller den han eller hon bestämmer) som får fatta beslut om begränsningar av tillgången till IT-system, inklusive sådana som använder Internet, samt tillgången till funktioner i IT-system. Om produktägaren vill inskränka privat användning i ett visst IT-system får detta endast göras från säkerhetssynpunkt och efter samråd med MUST.

15.1.5 Privat fillagring på Försvarsmaktens lagringsytor

CIO har beslutat [referens 22] att privat fillagring på Försvarsmaktens lagringsytor är tillåten endast vid användning av Försvarsmaktens e-post för privat bruk under förutsättning att det inte belastar Försvarsmaktens lagringsytor med mer än 10 MB per användare. Övrig användning för privat bruk är inte tillåten.

15.2 Användning av privata IT-system för tjänstebruk

Försvarsmakten ska naturligtvis se till att en anställd får den utrustning som behövs för att lösa tjänsteuppgifterna. En fråga som ofta uppkommer är om en anställd får utföra sina tjänsteuppgifter på en privat dator. Av Försvarsmaktens informationssäkerhetspolicy (bilaga 4) framgår att det övergripande målet med myndighetens informationssäkerhet är att säkerställa ett tillräckligt skydd för myndighetens informationstillgångar såväl inom som utom landet, så att rätt information är tillgänglig för rätt person i rätt tid på ett spårbart sätt. Det är svårt att uppnå ett sådant skydd för myndighetsinformation som behandlas eller lagras i ett privat IT-system. Vidare har Försvarsmakten naturligtvis inte heller någon rätt att utföra kontroller från säkerhetssynpunkt i sådana IT-system som innehas av en anställd som privat egendom.

Försvarsmakten måste således vara ytterst restriktiv med att låta en anställd använda sin privata dator för kontinuerligt tjänstebruk. Det är en avdelningschef eller motsvarande som bör fatta beslut om och under vilka former som en anställd får använda sitt privata IT-system (t.ex. en fristående dator, ett nätverk, en smart telefon eller en videokamera) för att regelbundet lösa sina tjänsteuppgifter. Ett sådant beslut bör beredas tillsammans med organisationsenhetens IT-säkerhetschef. En förutsättning för att låta en anställd använda sin privata dator är att den är utrustad med skydd mot skadlig kod. Ett privat IT-system får, utan beslut av avdelningschef eller motsvarande, användas för att lösa högst tillfälliga arbetsuppgifter.

För att kunna ansluta en privat dator till Försvarsmaktens IT-system måste systemet genom auktorisation och ackreditering (avsnitt 19) vara godkänt för en sådan anslutning. I övriga fall är en anslutning inte tillåten.

Det får naturligtvis inte förekomma uppgifter som omfattas av sekretess enligt OSL på ett privat IT-system eller ett privat lagringsmedium. Det är således inte tillåtet att över ett privat e-postkonto sända uppgifter som omfattas av sekretess enligt OSL. Att använda e-post och skicka okrypterade uppgifter är lika osäkert som att skicka ett vanligt vykort. Även om ett privat lagringsmedium inte innehåller uppgifter som omfattas av sekretess enligt OSL får det inte anslutas till Försvarsmaktens IT-system.

15.3 Distansarbete

Med distansarbete avses arbete som arbetstagaren bedriver utanför Försvarsmaktens objekt, lokaler och områden och som inte är den ordinarie arbetsplatsen. Exempelvis kan sådant arbete bedrivas i hemmet eller vid en annan särskild av arbetsgivaren anvisad plats. IT-säkerheten i ett IT-system som ska användas för distansarbete måste vara

anpassat för sådant arbete, t.ex. vad gäller skydd av lagringsmedier och anslutning till elektroniska kommunikationsnät.

Organisationsenheterna har små möjligheter att lokalt utveckla IT-system för distansarbete som har en tillräcklig IT-säkerhet. Sådana IT-system bör beställas och levereras centralt i Försvarsmakten.

Verksamhetens behov att använda ett visst IT-system för distansarbete bör framgå i en verksamhetsanalys för IT-systemet (avsnitt 14.2). Produktägarens syn på om ett IT-system kan användas för distansarbete bör framgå av IT-systemets auktorisationsunderlag.

15.4 E-post

När man skickar e-post till adresser inom Försvarsmaktens domäner skyddas informationen i e-posten av skyddet kring Försvarsmaktens nätverk (FM-IP nät). När e-posten däremot lämnar FM-IP nät (över ett s.k. öppet nätverk) har den inte samma skydd som inom FM-IP nätet. Hemliga uppgifter får naturligtvis inte sändas i ett IT-system som inte är avsedda för behandling av hemliga uppgifter.

Se avsnitt 10.3 om kryptering vid överföring av sekretessklassificerade uppgifter.

15.4.1 Spam

Det finns rättsliga och arkivmässiga möjligheter att införa filter som raderar eller särskiljer skräppost (spam) i Försvarsmakten. Möjligheterna har beskrivits i [referens 13] och återges nedan. I takt med att spam förändras, förändras även de produkter som utgör skydd mot spam. Då det finns behov av att över tid kunna ha rätt nivå på skyddet, har det utvecklats en de facto-standard för normaliserade skyddsnivåer, s.k. Spam Confidence Level (SCL). SCL ska användas i Försvarsmakten för att kategorisera och automatiskt välja åtgärder för att hantera spam [referens 38]. I [referens 38] anges vilka automatiserade åtgärder som får användas.

Till Försvarsmaktens organisationsenheter inkommer en stor mängd elektronisk post som helt saknar värde för myndigheten och som inte heller enligt vad som följer av bestämmelserna i förvaltningslagen kan anses vara av betydelse för avsändaren. Sådan post utgörs inte sällan av reklam som helt saknar samband med myndighetens verksamhet. Sådan skräppost, eller spam, utgör genom sin stora mängd ett hot mot tillgängligheten till myndighetens IT-system, och riskerar på sikt att andra och viktiga meddelanden fördröjs eller inte når fram till myndigheten. Spam kan dessutom innehålla skadlig kod.

Enligt bestämmelserna i 2 kap. TF är ett spam att bedöma som en handling (en upptagning). Sammanfattningsvis blir en upptagning en allmän handling hos en myndighet när en annan organisationsenhet i Försvarsmakten, en annan myndighet eller en enskild har gjort den tillgänglig för myndigheten. Spam är alltså allmänna handlingar.

En allmän handling får bara utplånas, förstöras eller på annat sätt göras permanent otillgänglig (gallras) hos en organisationsenhet i Försvarsmakten om Riksarkivet har meddelat ett s.k. gallringsbeslut beträffande det aktuella slaget av handling. I Riksarkivets föreskrifter om gallring av handlingar av tillfällig eller ringa betydelse finns gallringsföreskrifter som kan tillämpas i fråga om spam. Dessa föreskrifter förutsätter att Försvarsmakten meddelar tillämpningsbestämmelser. Sådana beslutades den 21 december 2005 [referens 17]. Det är alltså möjligt att gallra spam.

Det är viktigt att hålla i minnet att om ett meddelande innehåller information som på något sätt har betydelse för myndigheten, t.ex. om en enskild vill framföra synpunkter till myndigheten, är meddelandet inte att betrakta som spam. Detta gäller även om meddelandet inledningsvis har bedömts (klassificerats) som spam. Normalt ska all post som är avsedd för myndigheten läsas, oavsett om den kommer i pappersform eller t.ex. som ett e-postmeddelande. Med hänsyn till de enorma mängderna spam som inkommer till Försvarsmakten är det inte möjligt att manuellt bedöma om innehållet saknar värde för myndigheten. En manuell hantering skulle kräva sådana personella insatser att kostnaderna blir orimligt stora. Dessutom riskerar omfattningen av spam att blockera betydelsefulla meddelanden från att nå fram till myndigheten. Med hänsyn till att automatiserade processer (s.k. spam-filter) med en hög grad av tillförlitlighet kan avgöra om ett e-postmeddelande utgör spam är det inte heller av rättssäkerhetsskäl befogat med en manuell hantering.

Den vars e-postmeddelande till myndigheten har stoppats av ett spam-filter måste däremot kunna få godtagbar information om hur vederbörande i den aktuella situationen kan komma i kontakt med myndigheten. Det får anses godtagbart om myndigheten på sin webbplats på ett tydligt sätt upplyser om att e-post kan ha blivit spärrad. Ett sådant meddelande bör ha följande lydelse.

Försvarsmakten använder ett automatiskt säkerhetssystem för att skydda e-post-systemet mot vad som ofta benämns som skräppost (s.k. spam-filter). Om Ni utan framgång har försökt att komma i kontakt med myndigheten via ett e-postmeddelande kan det bero på att meddelandet har stoppats av säkerhetssystemet.

Om Ni vill komma i kontakt med myndigheten kan Ni försöka sända meddelandet på nytt eller skriva eller ringa till den organisationsenhet i myndigheten som Ni vill komma i kontakt med. Ni kan även skriva till Försvarsmaktens högkvarter, 107 85 STOCKHOLM eller ringa på telefon 08 - 788 75 00.

Texten i detta meddelande bör naturligtvis anpassas till aktuell organisationsenhet. Texten bör även återges på engelska.

Således finns det numera inga rättsliga eller arkivvårdsmässiga hinder för att införa spam-filter i Försvarsmakten. Ett sådant införande måste naturligtvis föregås av auktorisation.[318]

15.5 Sociala medier

Sociala medier är ett samlingsbegrepp för medier eller kanaler på Internet som skapar förutsättningar för kommunikation mellan människor. Några exempel är bloggar, webbforum och wikis. Exempel på sociala medier är tjänster som Wikipedia, Facebook, YouTube, Flickr, Twitter och WordPress.

Överbefälhavaren har beslutat Försvarsmaktens riktlinjer för sociala medier [referens 46]. Riktlinjerna reglerar Försvarsmaktens hantering av sociala medier. Riktlinjerna innehåller bestämmelser för myndighetens användning av sociala medier samt vissa bestämmelser för Försvarsmaktens personal, bl.a. följande.

- Försvarsmakten tillåter användning av sociala medier på arbetsplatsen i såväl privata som tjänsterelaterade syften, utom då den bryter mot myndighetens bestämmelser. Den privata användningen får inte vara av sådan omfattning att den inkräktar på användarens tjänsteutövning.
- Offentliga sociala medier utgör inte primärt kanaler för tjänstesamtal av olika slag mellan medarbetare. Den sortens internkommunikation stöds i stället av Försvarsmaktens intranät och andra interna IT-system.

318 6 § Försvarsmaktens interna bestämmelser om IT-verksamhet.

Användning av sociala medier medför risker, t.ex. för att uppgifter som omfattas av sekretess enligt OSL röjs. Sociala medier kan också användas av en underrättelseaktör i syfte att kartlägga människors bakgrund och intressen för att underlätta kontakttagning. Säkerhetskontoret har därför gett ut ett informationsblad [referens 30] och en informationsfolder [referens 32] om sociala medier och säkerhet.

16 Säkerhetskopiering

Säkerhetsskyddet ska bl.a. förebygga att hemliga uppgifter obehörigen röjs, ändras eller förstörs, oavsett om det sker uppsåtligen eller av oaktsamhet. I fråga om behandling av hemliga uppgifter i ett IT-system är det därför nödvändigt att de behandlade uppgifterna säkerhetskopieras så att de efter ett avsiktligt angrepp, olycka eller mänskligt felgrepp kan återställas. Förutom för säkerhetskopior av säkerhetsloggar innehåller Försvarsmaktens föreskrifter om säkerhetsskydd och Försvarsmaktens interna bestämmelser om IT-säkerhet inga föreskrifter om säkerhetskopiering. Riksarkivet har dock meddelat föreskrifter om säkerhetskopiering av elektroniska handlingar som gäller för en myndighet oavsett om uppgifter som behandlas omfattas av sekretess eller inte omfattas av sekretess.

> *Myndigheten ska regelbundet framställa säkerhetskopior av de elektroniska handlingarna. Säkerhetskopiorna ska omfatta samtliga handlingar som är allmänna.*
>
> *Säkerhetskopiering ska ske på ett sådant sätt och med sådan periodicitet att handlingarna kan återställas. Rutiner för säkerhetskopiering och för återställning av elektroniska handlingar ska dokumenteras i enlighet med 2 §.*
>
> *Säkerhetskopior ska förvaras geografiskt åtskilt från de kopierade elektroniska handlingarna.*
>
> 6 kap. 5 § Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling)

Av föreskriften följer att en *myndighet* ska låta säkerhetskopiering ingå i den analys av vilket säkerhetsskydd som ett IT-system, som är avsett för behandling av hemliga uppgifter, kräver och vilka åtgärder som måste vidtas för att säkerhetskopieringen ska få avsedd effekt.[319]

Av föreskriften följer att säkerhetskopiering *i Försvarsmakten* ska ingå i en säkerhetsmålsättning för ett IT-system, oavsett de behandlade uppgifternas informationsklassificering. Av säkerhetsmålsättningen ska framgå vilken säkerhetskopiering ett IT-system behöver och vilka åtgärder som måste vidtas för att säkerhetskopieringen ska få avsedd effekt.[319] [320] [321] Åtgärderna avser även rutiner för återläsning och test av återläsning.

319 7 kap. 7 och 9 §§ Försvarsmaktens föreskrifter om säkerhetsskydd.
320 1 kap. 2 § Försvarsmaktens interna betämmelser om IT-säkerhet.
321 4 kap. 1 och 4 §§ Försvarsmaktens interna bestämmelser om IT-säkerhet.

Föreskriften hänvisar till 6 kap. 2 § Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling). Den föreskriften avser en *plan* för hur de elektroniska handlingarna ska skyddas, dokumentation av de åtgärder och rutiner som vidtas samt kontroll av hur planen följs. Någon sådan plan eller kontroll behövs inte i Försvarsmakten då föreskriften motsvaras av föreskrifterna i:

- 7 kap. 7 § Försvarsmaktens föreskrifter om säkerhetsskydd (avsnitt 14.1 om säkerhetsmålsättning),
- 7 kap. 9 § Försvarsmaktens föreskrifter om säkerhetsskydd (avsnitt 13.6 om dokumentation av skyddet),
- 4 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet (avsnitt 14.1 om säkerhetsmålsättning),
- 4 kap. 4 § Försvarsmaktens interna bestämmelser om IT-säkerhet (avsnitt 13.6 om dokumentation av skyddet),
- 6 kap. 1 § Försvarsmaktens föreskrifter om säkerhetsskydd,
- 6 kap. 4 och 7 §§ Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel samt av
- 13 kap. 3 och 4 §§ Försvarsmaktens interna bestämmelser om IT-säkerhet.

Myndigheten ska säkerställa tillgången till sådan utrustning och programvara som behövs för att kunna återställa de elektroniska handlingarna. Utrustning och programvara ska förvaras geografiskt åtskilda från handlingarna.

6 kap. 6 § Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling)

I samband med utveckling och anskaffning av ett IT-system är det nödvändigt att säkerställa att utrustning och programvara finns på de platser som kan komma i fråga för att kunna återställa de säkerhetskopierade uppgifterna.

Som allmän handling anses inte handling som en myndighet förvarar endast i syfte att kunna återskapa information som har gått förlorad i en myndighets ordinarie system för automatiserad behandling av information (säkerhetskopia).

2 kap. 10 § andra stycket TF

Endast handlingar som förvaras i syfte att återskapa information som gått förlorad på grund av tekniska fel, sabotage, extraordinära händelser som brand eller översvämning m.m. omfattas av undantaget. Det är möjligt för en myndighet att återskapa information från en säkerhetskopia för att återställa information som av misstag har raderats. Återskapandet påverkar inte *säkerhetskopians* status som en handling som inte är allmän om säkerhetskopian fortfarande förvaras enligt det syfte som anges i föreskriften. Information som i ett sådant fall återskapats får bedömas enligt övriga regler i 2 kap. TF och kan på så sätt bli föremål för allmänhetens insyn.[322]

Om informationen i en säkerhetskopia bevaras även för andra ändamål än för att återskapa information som gått förlorad på grund av t.ex. tekniska fel eller brand faller säkerhetskopian utanför bestämmelsens tillämpningsområde, t.ex. om säkerhetskopian ska tas om hand för arkivering. Se exempel 16:1.

Exempel 16:1

Säkerhetskopior för IT-systemet XYZ förvaras i syfte att kunna återskapa information efter ett haveri. Säkerhetskopiorna är *även* den huvudsakliga platsen för förvaring av IT-systemets *säkerhetsloggar*. Syftet är att vid behov kunna använda säkerhetsloggarna vid utredningar.

Då säkerhetskopiorna inte endast förvaras i syfte att återskapa information som gått förlorad är säkerhetskopiorna allmänna handlingar.

Om rättsliga myndigheter använder sig av tvångsmedel för att få fram information som finns i en myndighets säkerhetskopior påverkar detta inte myndighetens ändamål med förvaringen. I sådana fall är *säkerhetskopian* fortfarande inte en allmän handling. Motsvarande gäller om information från en säkerhetskopia på begäran av en annan myndighet enligt 6 kap. 5 § OSL överlämnas till den andra myndigheten.

Såväl säkerhetskopior i form av t.ex. pappersutskrifter som lagringsmedier i IT-system omfattas av föreskriften.

En säkerhetskopia får i samband med begäran om utlämnande av allmän handling användas för att återskapa allmänna handlingar som av misstag har raderats.

322 Sidan 38, Säkerhetskopiors rättsliga status prop. 2009/10:58.

16.1 Skydd av säkerhetskopior

Myndigheten ska vid förvaring av elektroniska handlingar, säkerhetskopior och dokumentation tillämpa Riksarkivets föreskrifter och allmänna råd (RA-FS 1994:6) om planering, utförande och drift av arkivlokaler.

6 kap. 7 § Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling)

Föreskriften gäller för alla IT-system oavsett om IT-systemen är avsett för behandling av hemliga, utrikesklassificerade, sekretessklassificerade uppgifter eller uppgifter som inte omfattas av sekretess. RA-FS 1994:6 har ersatts av RA-FS 2013:4.

16.2 Förvaring av säkerhetskopierade säkerhetsloggar

Varje myndighet skall besluta vilket säkerhetsskydd som är erforderligt vad avser förvaring av säkerhetskopierade säkerhetsloggar.

7 kap. 12 § Försvarsmaktens förskrifter om säkerhetsskydd

Säkerhetsloggar är av betydelse för att i efterhand kunna rekonstruera händelseförlopp. De behöver därför särskilt skyddas.

Anledningen till att varje myndighet ska besluta om säkerhetsskyddet för förvaring av säkerhetskopierade säkerhetsloggar är att inga kopior ska få finnas på samma plats som originalen om t.ex. en brand bryter ut eller om någon tar sig in i lokalen och stjäl säkerhetsloggarna i någon avsikt. Det är inte enbart sekretessen för de registrerade händelserna som är av intresse, av stor betydelse är även säkerhetsloggens riktighet. Detta innebär att loggarna måste förvaras på ett sådant sätt att de kan skyddas dels mot obehörig åtkomst, dels mot förändring. Skyddet ska i denna del säkerställa att personal som arbetar i ett IT-system, t.ex. som behörighetsadministratör eller IT-tekniker, inte kan förändra en säkerhetslogg för att i efterhand dölja egna eller andras händelser i IT-systemet.

I 2 kap. 13-17 §§ Försvarsmaktens föreskrifter om säkerhetsskydd finns föreskrifter om förvaringsutrymmens skyddsnivåer. Vidare finns i 3 kap. 9-12 §§ Försvarsmaktens föreskrifter om säkerhetsskydd krav på vilka skyddsnivåer som gäller för t.ex. en datorhall.

17 Kommunikation mellan IT-system

I dessa bestämmelser avses med elektroniskt kommunikationsnät: system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.

1 kap. 6 § 5 Försvarsmaktens interna bestämmelser om IT-säkerhet

Definitionen på elektroniskt kommunikationsnät är ursprungligen hämtad från 1 kap. 7 § lagen om elektronisk kommunikation. Föreskriften avser bl.a. telefoni, bildöverföring och kommunikation i ett IT-system och mellan IT-system. Avsikten är att definitionen ska vara heltäckande.

Se avsnitt 12.4 för kommunikation mellan IT-system som sker med hjälp av flyttbara lagringsmedier.

17.1 Tillgänglighet i ett elektroniskt kommunikationsnät

Säkerhetsskyddet avser inte enbart att skydda hemliga uppgifter mot ett avsiktligt eller oavsiktligt röjande. Det är också viktigt att uppgifter i krislägen kan förmedlas till andra på ett betryggande sätt. I informationssäkerheten ingår därför även att se till att teleförbindelser och andra kommunikationsvägar håller en tillräckligt hög nivå från säkerhetssynpunkt.[323]

Om avsaknaden av tillgänglighet i ett elektroniskt kommunikationsnät kan påverka en myndighets verksamhet som är av betydelse för rikets säkerhet ska myndigheten vidta lämpliga säkerhetsskyddsåtgärder utifrån myndighetens säkerhetsanalyser avseende vilka hot, risker och sårbarheter som kan påverka sådan verksamhet.[324] I Försvarsmakten ska hot, risker och sårbarheter (inklusive avsaknaden av tillgänglighet) som kan påverka en organisationsenhets verksamhet analyseras för alla IT-system oavsett vilka uppgifter IT-systemen är avsedda att behandla.[325]

323 Sidorna 74-75, Säkerhetsskydd prop. 1995/96:129.
324 1 kap. 6 § Försvarsmaktens föreskrifter om säkerhetsskydd.
325 4 kap. 1 § andra stycket Försvarsmaktens interna bestämmelser om IT-säkerhet.

Behov av tillgängliga elektroniska kommunikationsnät bör för ett IT-system uppmärksammas genom verksamhetsanalys (avsnitt 14.2) och säkerhetsanalys (avsnitt 14.4). Ett sådant behov bör uppmärksammas oavsett vilka slag av uppgifter som IT-systemet är avsett att behandla. Krav på tillgängliga elektroniska kommunikationsnät kan formuleras som *tillkommande säkerhetskrav* (avsnitt 13.3) som ingår i en säkerhetsmålsättning (avsnitt 14.1) för ett IT-system. Åtgärder i samband med avbrott eller störningar i elektroniska kommunikationsnät ska för ett IT-system beskrivas i systemets kontinuitetsplanering (avsnitt 14.6) om ett avbrott eller en störning bedöms påverka IT-systemets funktion.[326]

Post- och telestyrelsen har gett ut en vägledning om anskaffning av robust elektronisk kommunikation [referens 35].

17.2 Anslutning av ett IT-system till ett elektroniskt kommunikationsnät

> *IT-system, som är avsedda för att användas för överföring av uppgifter via ett elektroniskt kommunikationsnät som har tillhandahållits av Försvarsmakten, får inte utan beslut av produktägaren kopplas till ett elektroniskt kommunikationsnät som inte har tillhandahållits av Försvarsmakten.*
>
> *IT-system, som inte är avsedda för att användas för överföring av uppgifter via ett elektroniskt kommunikationsnät som har tillhandahållits av Försvarsmakten, får användas för överföring av uppgifter till ett annat tillgängligt elektroniskt kommunikationsnät efter beslut av chefen för organisationsenheten.*
>
> *Beslut som avses i första och andra styckena ska dokumenteras.*
>
> 5 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Med ett elektroniskt kommunikationsnät som har *tillhandahållits av Försvarsmakten* avses:

- ett kommunikationsnät som ägs av Försvarsmakten eller
- ett kommunikationsnät som ägs av någon annan, t.ex. av ett företag, och som Försvarsmakten använder.

Det avgörande för om nätet är tillhandahållet av Försvarsmakten är om någon annan än Försvarsmakten får använda det.

Beslutsrätten enligt föreskriften får inte delegeras.

326 1 kap. 9 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

Det bör poängteras att det finns andra föreskrifter och beslut som måste följas för att få koppla ihop ett IT-system med ett elektroniskt kommunikationsnät, t.ex. beslut i fråga om ackreditering (kapitel 19). En anslutning av ett IT-system till ett elektroniskt kommunikationsnät kan endast få ske om det är förenligt med auktorisation och ackreditering av IT-systemet samt i enlighet med ägarföreträdarens bestämmelser. Den som ansvarar för ett elektroniskt kommunikationsnät kan ha ställt krav för hur nätet ska få användas, t.ex. i syfte att hushålla med kapacitet och för att inte olika IT-system ska påverka varandra eller nätet negativt. Kraven kan även direkt röra IT-säkerhet i IT-systemet. Sådana krav på IT-säkerhet bör tas med i regelverksanalysen (avsnitt 14.3) för IT-systemet.

Första stycket i föreskriften kan exemplifieras enligt följande.

Exempel 17:1

IT-systemet Lift-L är avsett för överföring av uppgifter via ett elektroniskt kommunikationsnät som har tillhandahållits av Försvarsmakten. I detta fall är kommunikationsnätet Försvarsmaktens IP-nät (FM IP-nät).

Om Lift-L ska kopplas till Internet, som är ett elektroniskt kommunikationsnät som inte har tillhandahållits av Försvarsmakten, får detta inte göras utan att produktägaren för Lift-L har beslutat om detta.

Oavsett val av elektroniskt kommunikationsnät måste produktägaren följa eventuella anslutningsbestämmelser till elektroniska kommunikationsnät som har tillhandahållits av Försvarsmakten. I detta exempel bör således produktägaren, innan han eller hon fattar sitt beslut, ta reda på vilka bestämmelser som gäller för anslutning till FM IP-nät.

Andra stycket i föreskriften kan exemplifieras enligt följande.

Exempel 17:2

Om det vid Högkvarteret finns en dator som ursprungligen inte är avsedd att anslutas till ett nätverk (elektroniskt kommunikationsnät) får datorn dock anslutas till t.ex. Internet efter beslut av chefen för Högkvarteret.

17.3 Dokumentation av ett elektroniskt kommunikationsnät

Produktägare och driftägare skall se till att det finns aktuella ritningar som beskriver de IT-system och elektroniska kommunikationsnät som var och en ansvarar för.

12 § Försvarsmaktens interna bestämmelser om IT-verksamhet

Sådana ritningar är även av betydelse för dokumentation över det skydd som finns i fråga om ett IT-system i Försvarsmakten, oavsett vilka slag av uppgifter som IT-systemet är avsett att behandla.[327] [328] [329]

327 7 kap. 9 § Försvarsmaktens föreskrifter om säkerhetsskydd.
328 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.
329 4 kap. 4 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

18 Säkerhetsfunktioner

I detta kapitel avses med säkerhetsfunktion: en eller flera funktioner i ett IT-system som upprätthåller säkerheten enligt regler om hur uppgifter i IT-systemet skall skyddas.

7 kap. 1 § 4 Försvarsmaktens föreskrifter om säkerhetsskydd

18.1 Godkännande av säkerhetsfunktioner

En myndighet som omfattas av Försvarsmaktens föreskrifter om säkerhetsskydd ska förse ett IT-system som är avsett för behandling av hemliga uppgifter med *av myndigheten godkända* säkerhetsfunktioner. Säkerhetsfunktionerna ska anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i ett sådant IT-system har placerats i.[330] [331] [332] [333] [334]

En myndighet måste således besluta vilka egenskaper respektive säkerhetsfunktion ska ha och under vilka förutsättningar en säkerhetsfunktion är godkänd vid en myndighet.

Vilka egenskaper som en myndighet väljer måste ske mot bakgrund av vilket säkerhetsskydd som behövs vid myndigheten med hänsyn till verksamhetens art, omfattning och övriga omständigheter.[335] Vidare måste en myndighet vid val av egenskaper särskilt beakta nya risker för förstörande eller röjande av hemliga uppgifter som finns i fråga om IT-system (se avsnitt 13.1 om säkerhetsskydd i och kring IT-system).[336]

18.2 Krav på godkända säkerhetsfunktioner i Försvarsmakten

För Försvarsmakten har MUST beslutat krav på godkända säkerhetsfunktioner (KSF 2.0 och 3.0) [referenserna 7, 9 och 44]. Vilka krav som ställs beror bl.a. på vilken högsta informationssäkerhetsklass som någon av uppgifterna i ett IT-system som säkerhetsfunktionerna ska skydda. I Försvarsmakten är det MUST som slutgiltigt i sitt ytt-

330 7 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd.
331 7 kap. 11 § Försvarsmaktens föreskrifter om säkerhetsskydd.
332 7 kap. 13 § Försvarsmaktens föreskrifter om säkerhetsskydd.
333 7 kap. 14 § Försvarsmaktens föreskrifter om säkerhetsskydd.
334 7 kap. 15 § Försvarsmaktens föreskrifter om säkerhetsskydd.
335 5 § första stycket säkerhetsskyddslagen.
336 9 § säkerhetsskyddslagen.

rande inför ackreditering avgör om säkerhetsfunktioner i ett IT-system är godkända (se kapitel 19 om ackreditering).[337]

Syftet med modellen för KSF är att på ett entydigt sätt definiera krav på de säkerhetsförmågor som ett visst system måste ha samt de assuranskrav som ger tilltro till att säkerhetsförmågorna existerar och att avsedda skyddsåtgärder därmed uppnås.

För anpassning av säkerhetskraven används i KSF 3.0 två faktorer:

1. Konsekvens av en oönskad händelse som påverkar sekretessen (informationsförlust) för informationen som bearbetas, lagras eller på annat sätt hanteras av systemet samt
2. hur exponerat systemet är för aktörer som kan påverka systemet.

I de fall där olika bedömningar kommer i konflikt med varandra sker avdömning genom dialog med MUST. Exempel på detta kan vara verksamhet där krav på tillgänglighet kommer i konflikt med krav på säkerhetsskydd.

KSF 3.0 innehåller:

- Metod för att fastställa kravnivå givet en viss miljö och användande, samt den i systemet hanterade informationens konsekvensnivå.
- Funktionella krav i olika nivåer för att erhålla ett balanserat skydd.
- Assuranskrav för att möjliggöra en verifiering av säkerheten.
- Beskrivning av en IT-säkerhetsspecifikation (ITSS, avsnitt 14.5), vilket är det dokument som innehåller underlag som är relevanta för ackreditering och verifiering av IT-systemet.
- Evalueringsmetodik för att få en viss kvalitet i granskningen av ITSS samt IT-säkerheten i systemet.

KSF 3.0 ska genom IT-säkerhetsspecifikationen och dess evaluering medge en kvalitetssäker bedömningsgrund för den vidare riskhanteringsprocessen där MUST bedömning ska visa på om systemet har eventuella kvarvarande risker (krav som inte är uppfyllda) och om den sammanlagda värderingen av skyddet ger att risknivån är acceptabel. KSF gör inga anspråk på fullständighet och det är därför som KSF benämns som minimikrav. IT-systemet måste fortfarande genomgå en verksamhetsanalys, regelverksanalys samt en säkerhetsanalys för att identifiera eventuella ytterligare krav. KSF ska tillsammans med krav från dessa analyser utgöra en komplett kravbild vad gäller informationssäkerhet.

337 12 kap. 4 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

Då man planerar att ta fram ett nytt IT-system är det viktigt att man gör de inledande analyserna och tidigt i projektet tar reda på vilket skydd som systemet kommer att behöva. Även om KSF inte pekar ut någon specifik arkitektur eller implementation som den enda rätta är många gånger den säkerhetsfunktionalitet som kravställs i KSF mer att jämföra med egenskaper hos IT-systemets arkitektur än specifika funktioner som går att lägga till i efterhand. Därför är det i många fall väldigt kostnadsdrivande att bygga till säkerhet i efterhand då stommen till systemet redan är fastställd.

Skyddet mot sekretessförlust och därmed också spårbarheten i Försvarsmaktens IT-system måste vara hög och framförallt jämt då det ska skydda mot en kvalificerad angripare som kommer att välja det enklaste sättet att försöka få tag i den information som han eller hon är intresserad av. En del av skyddet kring de egna systemen är att inte sprida information om hur det egna skyddet är beskaffat till en större krets är nödvändigt. Detta för att göra det svårare för en angripare att få information om eventuellt förekommande sårbarheter i säkerhetsskyddet. Avsnitt 3.4 i H Säk Sekrbed A beskriver säkerhets- och bevakningssekretess enligt 18 kap. 8 § OSL som även gäller för uppgifter om säkerhetsåtgärder i ett IT-system. Sådana uppgifter kan även omfattas av sekretess enligt 15 kap. 1 eller 2 §§ OSL.

Indelning av säkerhetsfunktioner är gjord för att skapa systematik i kravmassan. Säkerhetsfunktionerna är beroende av varandra för att fungera och många säkerhetsåtgärder som görs i IT-system kan därför vara svåra att passa in under någon specifik säkerhetsfunktion.

18.3 Behörighetskontroll

> *I detta kapitel avses med behörighetskontroll: administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att kontrollera en användare identitet, styra en användares behörighet att använda IT-systemet och dess resurser samt registrera användaren.*
>
> 7 kap. 1 § 3 Försvarsmaktens föreskrifter om säkerhetsskydd

Föreskrifterna om behörighetskontroll tillsammans med föreskrifterna om säkerhetsloggning (som beskrivs i avsnitt 18.4) avser främst att bemöta hot från behöriga användare och obehöriga personer som har tillgång till någon av IT-systemets gränsytor.

Säkerhetsfunktionen för behörighetskontroll syftar till att skydda information (uppgifter) och resurser så att dessa endast är tillgängliga för de som har rätt behörighet. Säkerhetsfunktionen behörighetskontroll går att dela upp i två delar, *autentisering* och *åtkomstkontroll*. Autentiseringen syftar till att säkerställa att en användare är den han eller hon utger sig för att vara och att denna är en registrerad, behörig användare till

IT-systemet. Åtkomstkontrollen syftar till att säkerställa att den autentiserade användaren har behörighet att ta del av resurserna i IT-systemet som han eller hon efterfrågar.

Säkerhetsfunktionen för säkerhetsloggning är beroende av att säkerhetsfunktionen för behörighetskontroll fungerar eftersom tilltron till genererade säkerhetsloggar aldrig kan bli högre än tilltron till säkerhetsfunktionen för behörighetskontroll.

För IT-system i Försvarsmakten som inte är avsedda för behandling av hemliga eller utrikesklassificerade uppgifter finns motsvarande definition i 1 kap. 6 § 6 Försvarsmaktens interna bestämmelser om IT-säkerhet.

Ett system som av flera personer skall användas för automatisk informationsbehandling av hemliga uppgifter skall vara försett med funktioner för behörighetskontroll och registrering av händelser i systemet som är av betydelse för säkerheten.

12 § andra stycket säkerhetsskyddsförordningen

I ett IT-system som ska användas av flera personer och som är avsett för behandling av hemliga uppgifter ska det finnas en funktion för behörighetskontroll som styr tillgången till IT-systemets resurser och säkerhetsloggning som loggar användarens åtkomst till resurserna.

18.3.1 Godkänd säkerhetsfunktion för behörighetskontroll

Varje IT-system som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer skall vara försett med en av myndigheten godkänd säkerhetsfunktion för behörighetskontroll. En sådan säkerhetsfunktion skall anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

7 kap. 10 § Försvarsmaktens föreskrifter om säkerhetsskydd

Se avsnitt 18.1 om en myndighets godkännande av säkerhetsfunktioner.

I Försvarsmakten gäller föreskriften även för IT-system som är avsedda för behandling av utrikesklassificerade uppgifter.[338]

338 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

I 7 kap. 10 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd föreskrivs att varje IT-system som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer ska vara försett med en av myndigheten godkänd säkerhetsfunktion för behörighetskontroll. Även övriga IT-system som är avsedda att användas av flera personer ska vara försedda med en sådan godkänd säkerhetsfunktion.

Med myndighet enligt första stycket avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

7 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Se avsnitt 18.2 om MUST godkännande av säkerhetsfunktioner i Försvarsmakten.

Föreskriften gäller för alla IT-system i Försvarsmakten oavsett vilka slag av uppgifter som IT-systemet är avsett att behandla, även i fråga om uppgifter som inte omfattas av sekretess enligt OSL.

Föreskriften gäller endast system som ska användas av fler än en person. Anledningen till att det inte krävs en godkänd säkerhetsfunktion för behörighetskontroll till ett IT-system som endast ska användas av en person är att en behörighetskontroll inte då fyller någon funktion. Det är då samma person som sköter säkerheten i IT-systemet respektive som använder systemet. Däremot kan säkerheten i ett IT-system med endast en användare utökas genom att systemet förses med en säkerhetsfunktion för behörighetskontroll som syftar till att skydda mot att någon som inte är behörig att använda IT-systemet kan bereda sig tillfällig tillgång till det.

Säkerhetsfunktionen för behörighetskontroll ska genom *administrativa* eller *tekniska* åtgärder, eller genom en *kombination* av sådana åtgärder, kontrollera en användares identitet, styra en användares behörighet att använda IT-systemet och dess resurser samt registrera användaren.[339] Säkerhetsfunktionen för behörighetskontroll behöver anpassas efter de förutsättningar som gäller för ett visst IT-system och de uppgifter som behandlas i IT-systemet. En sådan anpassning kan t.ex. avse om sluten eller öppen behörighetstilldelning ska användas (avsnitt 7.10). Säkerhetsfunktionen för behörighetskontroll för en publikt tillgänglig webbserver på Internet (exempel 18:1) och en databas för kvalificerat hemliga uppgifter har olika utformning.

339 7 kap. 1 § 3 Försvarsmaktens föreskrifter om säkerhetsskydd och 1 kap. 6 § 6 Försvarsmaktens interna bestämmelser om IT-säkerhet.

Exempel 18:1

En viss webbserver som är ansluten till Internet är avsedd för att allmänheten ska kunna läsa offentliga uppgifter om Försvarsmaktens olika verksamheter. När allmänheten läser innehållet på webbservern sker det anonymt. Allmänheten ska inte kunna ändra innehållet på de offentliga uppgifterna. I webbservern motsvaras allmänheten av en teknisk användare (användarnamn www) som endast har läsbehörighet till de offentliga uppgifterna.

Ett särskilt administrationsgränssnitt används av Försvarsmaktens personal som har till uppgift att hantera de offentliga uppgifterna på webbservern. Genom gränssnittet kan personalen efter inloggning ändra, lägga till och radera de offentliga uppgifterna.

Säkerhetsfunktionen för behörighetskontroll på webbservern är anpassad så att allmänheten anonymt kan läsa men inte ändra de offentliga uppgifterna. Försvarsmaktens personal kan på ett kontrollerat sätt hantera de offentliga uppgifterna.

Om kod eller kort eller båda ger behörighet till eller i ett IT-system ska kod respektive kort knytas till den individ som är behörig att använda eller ta del av uppgifter i systemet. Kod och kort ska hanteras på ett sådant sätt att någon obehörig person inte kan komma åt dem.

7 kap. 2 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Föreskriften begränsar inte säkerhetsfunktionen för behörighetskontroll till att endast använda kort eller kod eller båda för att autentisera användaren, även andra tekniker som t.ex. biometriska kan användas. Däremot följer det av paragrafen att om kod eller kort eller båda används, ska de vara individuella och hanteras så att inte någon annan än den kortet och eller koden tillhör kan komma åt dem.

I vissa fall finns det ett behov att låta flera personer kunna använda en kod eller kort för inloggning i ett IT-system, t.ex. rollkort för tjänst som vakthavande befäl. I sådana fall måste de personer som använder kod eller kort genom administrativa åtgärder knytas till koden eller kortet så att spårbarheten i efterhand är tillräcklig.

18.3.2 Autentisering

I steget autentisering ska användaren först presentera någon typ av unik identitet, t.ex. ett användarnamn, för att därefter bevisa att användaren är den rättmätiga ägaren

till identiteten. Det finns många sätt att göra detta på, vanligen används ett eller flera säkerhetsattribut av följande karaktärer:

- Något man är.
- Något man har.
- Något man vet.

I kategorin *något man är* räknar man in de biometriska teknikerna som ögonbottenavläsning, fingeravtryckskläsning och röstigenkänning. *Något man har* kan vara ett aktivt kort eller en dosa som kan förse autentiseringsfunktionen med ett engångslösenord. *Något man vet* är vanligen ett lösenord eller en pinkod.

Vilket sätt man ska använda sig av för att autentisera användare i ett IT-system bestäms av hur hög tilltro man behöver ha till autentiseringen i just det specifika IT-systemet. Hur hög tilltron måste vara i Försvarsmakten framgår av MUST krav på godkända säkerhetsfunktioner (KSF) [referens 44] som i sin tur bl.a. beror av den högsta informationssäkerhetsklassen som behörighetskontrollen ska skydda. I avsnitt 18.3.3 och 18.3.4 finns råd för användare som nyttjar olika säkerhetsattribut.

18.3.3 Lösenord

Det finns ett par råd som är mycket viktiga då man använder lösenord som säkerhetsattribut i säkerhetsfunktionen för behörighetskontroll.

Den absolut viktigaste tumregeln när man väljer ett lösenord är att välja något som *ingen* någonsin tidigare kan ha använt. Det vanligaste felet hos svaga lösenord är att de återanvänder vanliga ord och fraser som för en angripare blir lätta att gissa. Undvik därför enkla fraser som ”storgatan13B”, kluriga formuleringar som ”Äppelträd1” eller tangentborsmönster som ”!QA2ws3ed”.

Många lösenord går att forcera, skillnaden mellan ett bra och ett dåligt lösenord ligger i hur lång tid det tar att forcera det. Använd därför *inte* lösenord som innehåller:

- egennamn (t.ex. personer, sällskapsdjur, idrottslag, företag etc.),
- telefonnummer,
- geografiska namn,
- organisationsförkortningar,
- militära förkortningar,
- fordons registreringsnummer,
- personnummer,
- datum,

- annat sådant lösenord som kan härledas från användarens personliga förhållanden,
- namn eller förkortningar av namn på IT-system eller
- ord som finns i ordlistor (t.ex. ”lösen”, ”hemlig”, ”system”, ”master” eller ”password”).

Inte heller får lösenord enligt ovan skrivet baklänges användas.

Använd *aldrig* ett lösenord till mer än ett IT-system. En angripare som har gett sig tillgång till ett IT-system har mycket stora möjligheter att ge sig tillgång till fler IT-system om en användare nyttjar samma lösenord i flera IT-system. Ett lösenord måste alltid bestämmas av användaren utan att någon annan person ges möjlighet att ta del av detta.[340]

Ett nedtecknat lösenord ska förvaras med motsvarande skyddsnivå som de uppgifter eller den information som lösenordet ger tillgång till.[340] Risken för skrivavtryck på underliggande papper måste uppmärksammas.

Om ett IT-system har en funktion för slumpmässig generering av uttalbara lösenord kan en sådan funktion användas. Funktionen bör dock sortera bort ord som kan slås upp i en ordlista samt enkla repetitiva och systematiska mönster som t.ex. ”lalalala” och ”qwerty”.

Ett bra lösenord ska framförallt vara *långt*, idag är en vanlig rekommendation att det ska vara minst 16 tecken, men den siffran ändras i takt med teknikutvecklingen. Ett sätt att välja ett bra lösenord är att välja en fras, som gärna får innehålla ord ur flera språk, som t.ex. ”holaZezze,duserfantastisktpigguttoday”, eller ha felaktig meningsbyggnad och inte betyda någonting meningsfullt alls som t.ex. ”kokotjo!idetbluelingo nrisetyxskaft”. De angivna exempel får så klart inte väljas som lösenord.

Användaren kan när som helst, dock senast efter en viss i systemet angiven tid, byta lösenord. Tidigare använda lösenord eller lösenord som han eller hon använder eller har använt i andra IT-system måste undvikas. Byte av lösenord ska alltid göras när obehöriga inloggningsförsök noterats eller när misstanke föreligger om att lösenordet kan ha forcerats eller på något sätt kunnat komma till någon obehörig persons kännedom. Längsta giltighetstid för ett lösenord måste finnas dokumenterad. Generellt gäller att om ett lösenord måste bytas för ofta, tenderar användare ofta att inte tänka ut tillräckligt starka lösenord varje gång.

340 7 kap. 2 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

Ett lösenord till ett IT-system som är avsett för behandling av:

- sekretessklassificerade uppgifter eller
- uppgifter som inte omfattas av sekretess enligt OSL

omfattas av sekretess enligt 18 kap. 8 § 4 OSL. Ett sådant lösenord är i Försvarsmakten en sekretessklassificerad uppgift och ska omfattas av det skydd som föreskrivs i Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

18.3.4 Aktiva kort

I Försvarsmakten finns för närvarande två typer av kort för autentisering, Totalförsvarets elektroniska ID-kort (TEID) och Totalförsvarets aktiva kort (TAK). För att få tillgång till lokala rutiner kan man vända sig till sin lokala kortadministratör. En kortadministratör gör beställningar av aktiva kort och certifikat. Allmän information om hur man använder dessa kort, t.ex. hur och när man byter pinkoder, hur man förvarar dem och hur man ska agera vid en förlust finns beskrivet i H TST Grunder och I TST AKT.

18.3.5 Åtkomstkontroll

Efter att en autentisering av en användare i ett IT-system är genomförd kommer användaren automatiskt eller manuellt att begära tillgång till en eller flera av systemets tillgångar, t.ex. en hemlig uppgift som är lagrad i systemet. Då måste säkerhetsfunktionen för behörighetskontroll genom en åtkomstkontroll avgöra om användaren har behörighet till den efterfrågade tillgången och vilka dessa behörigheter är.

Det är av avgörande betydelse att en åtkomstkontroll genomförs för varje efterfrågad operation på en efterfrågad tillgång och inte bara första gången användaren begär åtkomst till tillgången.

En åtkomstkontroll kan implementeras genom användning av en eller en kombination av följande policys.

Åtkomstkontroll-policy	Beskrivning
Rollbaserad[341]	Utgår från att olika befattningar eller roller i organisationen har olika behörigheter i ett IT-system men att det finns en viss hierarki i organisationen. Det kan t.ex. vara att en chef ska ha behörighet att ta del av alla sina medarbetares jobb men de ska inte ha behörighet att se varandras. Man skapar därför roller med olika behörigheter till tillgångarna i systemet och till dessa roller knyts sedan användarna. Rollerna kan vara hierarkiskt uppbyggda och en användare kan tillskrivas mer än en roll. Denna typ av behörighetstilldelning är relativt lätt att administrera.
Regelstyrd[342]	Uppgifter i IT-systemet kodas eller märks med uppgift om informationsklassificering (avsnitt 13.10). En användare ges åtkomst endast om användaren i säkerhetsfunktionen för behörighetskontroll har definierats vara behörig att ta del av uppgifter tillhörande en viss informationsklassificering, t.ex. behörig att få ta del av uppgifter som är placerade i informationssäkerhetsklass HEMLIG/TOP SECRET (avsnitt 7.3).
Användarstyrd[343]	Den användare som skapar information i ett IT-system är den som tilldelar rättigheter till de användare som ska få ta del av eller ändra informationen.

18.3.6 Behörighet i IT-system

Grunder för behörighet beskrivs i kapitel 7.

> *Chefen för en organisationsenhet eller den han bestämmer ska besluta vem som är behörig att använda eller ta del av uppgifter i ett IT-system. Ett sådant beslut ska dokumenteras.*
>
> 7 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Det är inte lämpligt att delegeringen av rätten att besluta enligt föreskriften sker till en befattning på alltför låg nivå. En delegering bör inte göras längre än till den som är närmaste chef över den som avses beslutas att vara behörig, eftersom det oftast är den närmaste chefen som avgör vilka uppgifter som den anställde är behörig att ta del av för att den anställde ska kunna lösa sina arbetsuppgifter.

341 Motsvarar role-based access control (RBAC).
342 Motsvarar mandatory access control (MAC).
343 Motsvarar discretionary access control (DAC).

Om den som tilldelar en användare behörigheter i ett IT-system inte är samma person som beslutar om en person ska tilldelas behörighet är det nödvändigt att det finns en rutin som beskriver hur dessa två roller ska kommunicera med varandra för att tilldela och ta bort behörigheter i systemet.

När en anställning ändras, t.ex. vid byte av befattning eller ändring av organisatorisk tillhörighet, bör det återspeglas i en ändring av behörigheter i de IT-system som den anställde är användare i. En reducering av behörigheter bör övervägas innan en anställning upphör.

Rutiner för tilldelning, ändring och borttagning av behörighet bör framgå av organisationsenheternas och driftägarens systemspecifika IT-säkerhetsinstruktioner (avsnitt 14.8).

18.3.7 Borttagande av behörighet

En organisationsenhet bör ta fram riktlinjer för hur behörighet till ett IT-system tas bort. Det kan t.ex. finnas en checklista för avslutande av anställning där även borttagande av behörighet till IT-system finns med.

Borttagande av behörighet till ett IT-system bör ske genom att kontot ifråga spärras för inloggning. I de fall kontot i fråga tas bort innebär det att full spårbarhet inte alltid kan garanteras.

Ett IT-system bör vara försett med en automatisk spärrning av användarkontot om användaren inte varit inloggad under en definierad tid. Rutiner för borttagning av behörighet bör framgå av organisationsenheternas och driftägarens systemspecifika IT-säkerhetsinstruktioner (avsnitt 14.8).

18.3.8 Samma behörighet

I ett IT-system som inte är avsett för behandling av hemliga eller utrikesklassificerade uppgifter och där samtliga användare har beslutats vara behöriga till samtliga uppgifter behöver säkerhetsfunktionen för behörighetskontroll inte ingå i IT-systemets programvara. Det måste dock säkerställas att motsvarande skydd kan fås med andra tekniska eller administrativa funktioner.

Ett sådant motsvarande skydd kan uppnås genom att begränsa vilka personer som kan ge sig tillträde till det utrymme där IT-systemet är placerat (exempel 18:2).

Exempel 18:2

Ett IT-system är placerat i ett utrymme. Till utrymmet sker inpassering där personer är unikt identifierade i ett passerkontrollsystem. Endast personer som är beslutade att vara användare i IT-systemet har beslutats ha tillträdesrätt till utrymmet. Säkerhetsfunktionen för behörighetskontroll behöver inte ingå i IT-systemets programvara då motsvarande skydd uppnås med tillträdesrätten som upprätthålls med passerkontrollsystemet till utrymmet.

Se även avsnitt 13.4 om tillträdesbegränsning kring ett IT-system. I kapitel 5 i H SÄK Skydd beskrivs tillträdesbegränsning.

18.3.9 Systemadministratörens inloggning

Ett ordinarie systemadministratörskonto är inte alltid knutet till en specifik individ. I sådana fall bör ett sådant konto förses med ett tudelat lösenord och unika systemadministratörskonton skapas för varje administratör i systemet. Spärrning görs i närvaro av de personer som har tilldelats rollen som systemadministratör enligt följande rekommenderade rutin.

1. En kopia av administratörskontot görs där användaridentiteten eller kontot ges ett annat namn. Detta konto ges samma rättigheter som det ordinarie administratörskontot. Om det finns flera personer i organisationen som ska ha denna roll, ska ett sådant konto skapas för varje individ. Varje individs personliga aktiva kort eller lösenord kopplas sedan ihop med det nya kontot. De systemadministrativa åtgärder som han eller hon vidtar kommer att loggas på detta konto.
2. Kontot ”root”, ”administratör” eller motsvarande spärras genom byte av lösenord till kontot. De två personer som väljer varsin halva av lösenordet skriver ned detta var för sig och lägger dessa halvor i en förslutningspåse som förvaras tillsammans med andra reservnycklar och -koder.
3. Då en systemadministratör ska använda sin administratörsbehörighet för åtgärder, loggar personen in med sin användaridentitet till sitt administratörskonto. På så sätt kan loggningen av åtgärderna hänföras till denna användaridentitet. För normal användning (icke systemadministrativ användning) bör administratörer ha ett vanligt konto utan administrationsrättigheter som andra användare i IT-systemet.

En behörighetsadministratör och en administratör för säkerhetsloggar får inte ha samma behörigheter i ett IT-system. En behörighetsadministratör får inte ha behörighet att ändra eller radera säkerhetsloggar och en administratör för säkerhetsloggar

får inte ha behörighet att förändra sin egen eller andras behörigheter i IT-systemet (se även avsnitt 18.4 om administration av säkerhetsloggar).

18.3.10 Gallring av handlingar som rör behörighet

Föreskrifter om gallring av handlingar rörande säkerheten i och kring IT-system finns i Riksarkivets föreskrifter om gallring hos myndigheter under Försvarsdepartementet. Följande gallringsfrister gäller för handlingar som rör behörighet.[344]

Slag av handling		Gallringsfrist
Anteckningar om nytt lösenord		När de inte behövs i verksamheten
Tilldelning av användaridentiteter - beslut	Kvalificerat hemliga	25 år
	Hemliga	10 år
	Övriga	När de inte behövs i verksamheten
Registrering av användaridentitet	Kvalificerat hemliga	25 år
	Hemliga	10 år
	Övriga	När de inte behövs i verksamheten

18.4 Säkerhetsloggning

I detta kapitel avses med säkerhetsloggning: manuell eller automatisk registrering, eller både manuell och automatisk registrering, av händelser som är av betydelse för säkerheten i eller kring ett IT-system.

7 kap. 1 § 5 Försvarsmaktens föreskrifter om säkerhetsskydd

Säkerhetsfunktionen säkerhetsloggning riktar sig mot hot från behöriga användare eller obehöriga personer som har tillgång till någon av IT-systemets gränsytor. Säkerhetsloggning är ett sätt att möta hot genom att i säkerhetsloggen registrera vilka händelser som inträffar i IT-systemet som är av betydelse för säkerheten. En säkerhetslogg ska visa var, när och hur en händelse har inträffat och av vem åtgärden utfördes.

I Försvarsmakten används säkerhetsloggning för fortlöpande säkerhetskontroll i ett IT-system. En säkerhetslogg tjänar som underlag vid utredning av felaktig eller obehörig

344 2 § Riksarkivets föreskrifter om gallring hos myndigheter under Försvarsdepartementet.

användning och intrångsförsök. Därigenom kan säkerhetsloggen också utgöra en trygghet för behöriga användare mot ogrundade misstankar. Det kan dessutom krävas att man i efterhand, ibland efter lång tid, genom säkerhetsloggarna ska kunna rekostruera ett händelseförlopp. Vetskapen om att säkerhetsloggning sker i ett IT-system har i sig en avhållande effekt mot missbruk av systemet.

Aktiviteter loggas i säkerhetsloggar för att kunna:

- fria oskyldiga och avgränsa misstänkta,
- upptäcka händelser som utgör eller kan utgöra ett hot,
- avvärja fortsatt hot genom att vidta korrekta åtgärder,
- utreda inträffade händelser,
- bedöma eventuella skadeverkningar genom skade- och menbedömningar, och
- peka ut otillbörligt ändrade eller raderade filer så att dessa kan återskapas från en säkerhetskopia.

Ett annat syfte med säkerhetsloggningen är att den kan fungera som en kvittens på att en användare har tagit emot en hemlig handling i elektronisk form. Säkerhetsloggningen kan i sådana fall vara en elektronisk motsvarighet till kvittering vid mottagande av en hemlig handling (avsnitt 9.9). Säkerhetsloggningen uppfyller i denna del några av de *tillkommande säkerhetskrav* som följer av portalparagrafen 7 kap. 2 § Försvarsmaktens föreskrifter om säkerhetsskydd (avsnitt 13.3).

Säkerhetsfunktionen för säkerhetsloggning är beroende av andra säkerhetsfunktioner. Exempelvis kan tilltron till säkerhetsloggning aldrig bli större än den till säkerhetsfunktionen för behörighetskontroll eftersom det är behörighetskontrollen som knyter en viss händelse till en viss användare. Dessutom krävs att säkerhetsfunktionen för behörighetskontroll kan leverera en behörighetshistorik för samtliga användare av IT-systemet. Säkerhetsloggning är också beroende av säker tid i hela det övervakade IT-systemet för att händelser i olika delar av IT-systemet i efterhand ska gå att utläsa i kronologisk ordning.

Ett system som av flera personer skall användas för automatisk informationsbehandling av hemliga uppgifter skall vara försett med funktioner för behörighetskontroll och registrering av händelser i systemet som är av betydelse för säkerheten.

12 § andra stycket säkerhetsskyddsförordningen

I ett fleranvändarsystem som är avsett för behandling av hemliga uppgifter ska det finnas funktion för säkerhetsloggning som loggar användarens åtkomst till resurserna i IT-systemet.

> *I dessa bestämmelser avses med säkerhetslogg: behandlingshistorik över händelser som är av betydelse för säkerheten i eller kring ett IT-system.*
>
> 1 kap. 6 § 9 Försvarsmaktens interna bestämmelser om IT-säkerhet

I allmänhet loggas händelser i ett IT-system i flera loggfiler. De loggfiler som registrerar händelser av betydelse för IT-systemets säkerhet är säkerhetsloggar. I säkerhetsloggen ska samtliga händelser av betydelse för säkerheten i aktuellt IT-system registreras. Detta gäller även för händelser som inträffar i IT-systemets övriga säkerhetsfunktioner.

18.4.1 Godkänd säkerhetsfunktion för säkerhetsloggning

> *Varje IT-system som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer skall vara försett med en av myndigheten godkänd säkerhetsfunktion för säkerhetsloggning. En sådan säkerhetsfunktion skall anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.*
>
> 7 kap. 11 § Försvarsmaktens föreskrifter om säkerhetsskydd

Se avsnitt 18.1 om en myndighets godkännande av säkerhetsfunktioner.

I Försvarsmakten gäller föreskriften även för IT-system som är avsedda för behandling av utrikesklassificerade uppgifter.[345]

Föreskriften avser endast säkerhetsloggar vilket innebär att en myndighet kan avgöra vilken annan loggning utöver säkerhetsloggning som är av intresse för verksamheten men som inte ska loggas p.g.a. säkerhetsskäl. En transaktionslogg i en databashanterare och loggar för driftstatistik är exempel på loggar som inte behöver vara en säkerhetslogg.

Föreskrifterna om säkerhetsloggning är tillsammans med behörighetskontroll avsedda att skydda myndighetens uppgifter på insidan av ett IT-system. Föreskriften är begränsad till IT-system som endast används av flera personer. Ett enanvändarsystem omfat-

345 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

tas inte då det förutsätts att endast en person har tillgång till ett sådant IT-system och att det inte får kommunicera med något annat IT-system, varför säkerhetsrelaterade händelser sannolikt härrör från den enda användaren. Det skulle heller inte vara någon säkerhetshöjande åtgärd att den enda användaren i ett sådant IT-system även hanterar systemets säkerhetsloggar.

I 7 kap. 11 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd föreskrivs att varje IT-system som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer ska vara försett med en av myndigheten godkänd säkerhetsfunktion för säkerhetsloggning. Även övriga IT-system som är avsedda att användas av flera personer ska vara försedda med en sådan godkänd säkerhetsfunktion.

Med myndighet enligt första stycket avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

8 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Se avsnitt 18.2 om MUST godkännande av säkerhetsfunktioner i Försvarsmakten.

Föreskriften gäller för alla IT-system i Försvarsmakten oavsett vilka slag av uppgifter som IT-systemet är avsett att behandla, även i fråga om uppgifter som inte omfattas av sekretess enligt OSL. Föreskriften gäller enbart för IT-system som ska användas av flera personer.

Om produktägaren däremot väljer att även förse ett *enanvändarsystem* (avsnitt 13.9) med en säkerhetsfunktion för säkerhetsloggning måste systemet också förses med en säkerhetsfunktion för behörighetskontroll för att få avsedd effekt (exempel 18:3).

Exempel 18:3

I IT-systemet XYZ, som är ett enanvändarsystem, får endast tilldelade USB-minnen användas för säkerhetskopiering. Anslutningar av andra lagringsmedier är inte tillåtna. Produktägaren för IT-systemet har valt att använda säkerhetsloggning så att det i efterhand ska vara möjligt att undersöka vilka lagringsmedier som har anslutits till IT-systemet. För att skydda säkerhetsloggen mot obehörig påverkan används säkerhetsfunktionen behörighetskontroll.

18.4.2 Avstängning av säkerhetslogg

En säkerhetslogg får stängas av endast om det är oundgängligen nödvändigt.

Anledningen till avstängningen, vem som har fattat beslutet, tidpunkten för avstängningen och, om så har skett, tidpunkten för återstarten av loggen ska dokumenteras.

8 kap. 2 § Försvarsmaktens interna bestämmelser om IT-säkerhet

I föreskriften anges inte vem som får stänga av säkerhetsloggen. Det är inte rimligt att ange vem som får stänga av den, eftersom det kan uppstå situationer då säkerhetsloggarna måste stängas av för att förhindra en systemkrasch, t.ex. om en lagringsytas lagringskapacitet håller på att ta slut. I ett sådant läge är det viktigare att säkerhetsloggarna stängs av samt att detta dokumenteras än att det är en viss person som gör det enligt ett bemyndigande – d.v.s. alla tänkbara åtgärder vidtas för att förhindra en systemkrasch.

Ett IT-systems IT-säkerhetsinstruktion (avsnitt 14.8) bör beskriva i vilka lägen en person får stänga av en säkerhetslogg och i vilka fall man istället ska stänga av hela eller delar av IT-systemet. Ett exempel på det senare är om det finns misstanke att någon avsiktligt fyller säkerhetsloggarna för att dölja ett angrepp.

18.4.3 Analys av säkerhetslogg

För att fylla sin funktion krävs inte bara att händelser registreras i en säkerhetslogg, utan även att analys av registrerade händelser genomförs. Med analys avses all form av läsning och uttolkning av säkerhetsloggens innehåll.

För största möjliga flexibilitet vid logganalysen kopieras loggposterna lämpligen in i en relationsdatabas. I samband med detta kan även filtrering av loggposter ske så att endast säkerhetsrelevant information kopieras in i säkerhetsloggen. En logg i ett IT-system innehåller normalt ofta en stor mängd information, som inte är direkt relaterad till säkerheten i IT-systemet. Vad som kan filtreras bort och vad som ska finnas kvar, d.v.s. säkerhetsrelevant information, framgår av produktägarens beslut. Loggposter bör arkiveras i originalformat för att säkerställa trovärdigheten, t.ex. vid ett utredningsförfarande.

Beroende på de i IT-systemet behandlade uppgifternas placering i informationssäkerhetsklass och andra säkerhetskrav på IT-systemet, måste även larm kunna genereras när vissa säkerhetspåverkande händelser inträffar. Detta kan ske med hjälp av automatisk logganalys i samband med att loggposter skrivs till databasen.

Produktägaren ska se till att säkerhetsloggen kan analyseras och att loggen har erforderlig detaljeringsgrad.

8 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Föreskriften innebär inte att det är produktägaren som själv ska analysera en säkerhetslogg. Produktägaren ska se till att den kan analyseras.

De flesta operativsystem tillhandahåller funktioner som möjliggör läsning av säkerhetsloggar. Dessutom krävs det att en person analyserar resultaten. Den person som ska analysera en säkerhetslogg måste ha mycket god kännedom om t.ex. den trafik som säkerhetsloggas, för att på så sätt kunna upptäcka anomalier i det som loggas. Således måste en säkerhetslogg läsas och tolkning av dess innehåll måste genomföras.

Det kan även rekommenderas att det bör vara två av varandra oberoende personer som utför analysen. Om det endast är en person som utför analysen kan han eller hon utföra oegentligheter utan att det upptäcks. Dessutom undanröjer det misstankar om oegentligheter mot den enskilde personen.

Systemägaren eller den han bestämmer ska se till att säkerhetsloggar analyseras.

8 kap. 4 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Föreskriften innebär inte att det är systemägaren eller den han eller hon bestämmer som själv ska analysera säkerhetsloggarna. Denne ska *se till* att säkerhetsloggarna analyseras.

Systemägaren eller den han bestämmer ska minst enligt vad produktägaren har bestämt se till att säkerhetsloggarna analyseras. Även systemägaren kan ha ett intresse i analys av säkerhetsloggar. Det är sannolikt att systemägaren i dialog med produktägaren kommer att bestämma att det ankommer på driftägaren att analysera säkerhetsloggarna, eftersom säkerhetsloggarna finns i driftägarens verksamhet.

I det fall rollen systemägare inte ska finnas för ett IT-system (avsnitt 2.2.4) är det produktägaren som bör se till att säkerhetsloggar analyseras.

18.4.4 Information om säkerhetsloggning till användare

Chefen för organisationsenheten ska se till att användare av ett IT-system informeras om att säkerhetsloggning sker.

8 kap. 5 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Syftet med föreskriften är att en användare av ett IT-system ska vara informerad om att händelser som är av betydelse för säkerheten registreras och är föremål för kontroll. Ansvaret för att användarna är informerade om att säkerhetsloggning sker, åligger chefen för organisationsenheten.

Informationen bör ges i samband med utbildning av användare innan de får börja använda ett IT-system. Informationen bör även anges i IT-systemet som en upplysning till användarna i samband med inloggning.

18.4.5 Skydd och vård av en säkerhetslogg

Se avsnitt 16.2 om krav på förvaring av säkerhetskopierade säkerhetsloggar som gäller för såväl en myndighet som för en organisationsenhet i Försvarsmakten.

Varje säkerhetslogg vid organisationsenheten ska förvaras i läsbar form. Den ska fortlöpande kopieras och vårdas.

8 kap. 6 § Försvarsmaktens interna bestämmelser om IT-säkerhet

En säkerhetslogg ska förvaras så att uppgifternas tillgänglighet är säkerställd under hela bevarandetiden, d.v.s. tiden fram till dess att gallringsfristen löper ut.

Vad som avses med *läsbar form* är beroende av om händelserna har registrerats manuellt eller automatiskt. En säkerhetslogg kan vara manuell eller automatisk registrering eller både och.[346] Om händelserna har registrerats i elektronisk form avses med läsbar form att registrerade händelser i säkerhetsloggen måste *kunna* analyseras med ett tekniskt hjälpmedel (t.ex. ett logganalysverktyg). Om en säkerhetslogg lagras i elektronisk form måste den vara strukturerad på så sätt att de kan förväntas förbli läsbara, förståeliga och återsökningsbara under hela bevarandetiden.

346 7 kap. 1 § 5 Försvarsmaktens föreskrifter om säkerhetsskydd och 1 kap. 6 § 8 Försvarsmaktens interna bestämmelser om IT-säkerhet.

En säkerhetslogg måste under hela bevarandetiden dessutom kunna överföras till nya lagringsmedier, t.ex. för att kunna analyseras i ett annat IT-system som är avsett för verktygsbaserad analys av de registrerade händelserna.

18.4.6 Gallring av en säkerhetslogg

Föreskrifter om gallring av handlingar rörande säkerheten i och kring IT-system finns i Riksarkivets föreskrifter om gallring hos myndigheter under Försvarsdepartementet. I föreskriften framgår bl.a. följande gallringsfrister.[347]

Slag av säkerhetslogg	Gallringsfrist
Kvalificerat hemliga	25 år
Hemliga	10 år
Som utgör obligatoriskt räkenskapsmateriel	10 år
Övriga	När de inte behövs i verksamheten.

18.5 Skydd mot röjande signaler

> *I detta kapitel avses med röjande signaler: inte önskvärda elektromagnetiska eller akustiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs.*
>
> 7 kap. 1 § 6 Försvarsmaktens föreskrifter om säkerhetsskydd

Föreskrifterna om skydd mot röjande signaler (RÖS) är avsedda att i första hand skydda mot aktörer som aktivt genomför teknisk inhämtning genom avlyssning av röjande signaler från en myndighets anläggningar och kommunikationer. Syftet med säkerhetsfunktionen skydd mot röjande signaler är att eliminera eller kraftigt begränsa effekten för en aktör som genomför en sådan inhämtning.

För att en signal ska vara en röjande signal så ska den ha förmågan att bära information. En informationsbehandlande utrustning kan alstra stora mängder elektromagnetiska eller akustiska signaler utan att signalerna är röjande signaler eftersom signalerna inte innehåller någon information.

En informationsbehandlande utrustning kan också avge röjande signaler i form av en elektrisk signal som överlagras på en elektrisk ledare, t.ex. strömförsörjning och kommunikationskablage, som är anslutna till utrustningen, s.k. ledningsbunden RÖS.

347 2 § Riksarkivets föreskrifter om gallring hos myndigheter under Försvarsdepartementet.

För att förhindra att uppgifter som behandlas i ett IT-system från att röjas genom röjande signaler, minimeras generellt den elektromagnetiska strålningen genom att dämpa den utsända signalen eller välja komponenter och utrustning med goda skyddsegenskaper mot röjande signaler. Dämpning av ledningsbundna signaler utförs med hjälp av filtrering. Genom att komplettera filtreringen med en metallisk inkapsling skapas en heltäckande elektromagnetisk skärm, s.k. Faradays bur. När utrustning konstrueras kan konstruktionsprinciper användas för att minska de röjande signalerna. Dämpning av röjande signaler kan göras direkt på ett kretskort för den komponent på kortet som alstrar signaler eller med en elektromagnetisk skärm för hela eller delar av utrustningen. Dämpning kan även åstadkommas genom att tillföra material som har egenskapen att absorbera signalerna.

Röjande signaler i akustisk form dämpas med tekniker för att skydda mot obehörig avlyssning i en lokal eller ett område.

”TEMPEST” är en vanlig benämning hos andra stater som motsvarar röjande signaler. En djupare beskrivning av röjande signaler finns i broschyren *RÖS Röjande signaler – uppkomst, utbredning, skyddsmetoder, krav* som är utgiven av FMV (bilaga 1 innehåller referens till broschyren). I broschyren beskrivs även vissa utländska TEMPEST-bestämmelser.

18.5.1 Godkänd säkerhetsfunktion för skydd mot röjande signaler

Varje IT-system som är avsett för behandling av hemliga uppgifter skall vara försett med av myndigheten godkända säkerhetsfunktioner för skydd mot röjande signaler och obehörig avlyssning. Sådana säkerhetsfunktioner skall anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

IT-system som är avsedda för behandling av uppgifter som har placerats i högst informationssäkerhetsklassen HEMLIG/RESTRICTED behöver dock inte förses med en säkerhetsfunktion för skydd mot röjande signaler.

7 kap. 13 § Försvarsmaktens föreskrifter om säkerhetsskydd

Se avsnitt 18.1 om en myndighets godkännande av säkerhetsfunktioner.

I Försvarsmakten gäller föreskriften även för IT-system som är avsedda för behandling av utrikesklassificerade uppgifter.[348]

348 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Med myndighet som enligt 7 kap. 13 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd ska godkänna säkerhetsfunktioner för skydd mot röjande signaler och obehörig avlyssning avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

9 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Se avsnitt 18.2 om MUST godkännande av säkerhetsfunktioner i Försvarsmakten.

Vilka krav som gäller i Försvarsmakten för säkerhetsfunktionen skydd mot röjande signaler framgår av bilaga 1 till [referens 14].

18.5.2 Utrustningsklasser

I Försvarsmakten finns tre utrustningsklasser benämnda U1, U2 och U3. Utrustningsklasserna används för att kategorisera utrustning som har kända RÖS-egenskaper. Utrustningen märks med etiketter (bild 18:1, bild 18:2 och bild 18:3) som visar vilken utrustningsklass de har placerats i.

Utrustningsklass 1 (U1) är konstruerad så att den röjande signalen i princip är eliminerad. På denna typ av utrustning är RÖS-säkerhetsavståndet mycket kort.

Utrustningsklass 2 (U2) används då man inte har lika höga krav på skydd. Den röjande signalen från utrustning i denna klass når betydligt längre är för utrustning i klass U1 men är dock begränsad.

Utrustningsklass 3 (U3) är en märkning man använder på utrustning som inte uppfyller något av kraven för utrustningsklass 1 eller 2 men där utrustningen är mätt och dess RÖS-säkerhetsavstånd är känt. Det behöver inte betyda att utrustningen har goda RÖS-egenskaper. Utrustning i utrustningsklass 3 måste ofta användas på ett speciellt sätt eller i en viss fast konfiguration för att de uppmätta RÖS-egenskaperna ska gälla. Etiketten för U3 har därför utrymme för att kunna ge en referens till de föreskrifter som gäller för den aktuella utrustningen.

Bild 18:1 - *Etikett för utrustningsklass 1.*

Bild 18:2 - *Etikett för utrustningsklass 2.*

Bild 18:3 - *Etikett för utrustningsklass 3.*

En RÖS-godkänd utrustning är också plomberad för att det ska vara svårare att manipulera utrustningen utan att användaren blir uppmärksammad på det. Plomberingsetiketterna sätts på ett sådant sätt att förseglingen kommer att brytas om utrustningen öppnas (bild 18:4 och bild 18:5).

Godkännandet av RÖS-mätt utrustning gäller enbart den konfiguration som utrustningen hade då den mättes och godkändes. Extrautrustning, t.ex. hörlurar och USB-tillbehör kan, om de inte är godkända ur RÖS-synpunkt agera som antenner och kraftigt förstärka även en mycket svag röjande signal.

Bild 18:4 *- Röd plomberingsetikett används för utrustning som endast får användas inom svenskt territorium.*

Bild 18:5 *- Blå plomberingsetikett används för utrustning som får användas även utanför svenskt territorium.*

18.5.3 Skalskyddsklasser

I Försvarsmakten finns två skalskyddsklasser benämnda SS1 och SS2 vilka man använder för att beskriva RÖS-egenskaperna hos en RÖS-skyddad lokal eller ett kabinett.

Skalskyddsklass 1 (SS1) är konstruerad så att den röjande signalen från utrustningen i rummet i princip är eliminerad utanför dess väggar.

Skalskyddsklass 2 (SS2) används då man inte har lika höga krav på skydd. I denna klass är dämpningen i rummets väggar inte lika bra som för SS1 men ändå betydande.

För att kontrollera att skyddet i en RÖS-skyddat utrymme blir vad man förväntade sig vid byggnationen utförs alltid en dämpningsmätning av utrymmet innan utrymmet tas i bruk. Efter en förändring av eller i ett sådant rum görs alltid en analys av förändring för att avgöra om förändringen kan ha påverkat rummets RÖS-egenskaper negativt. Om analysen inte kan utesluta att rummets RÖS-egenskaper har påverkats negativt så görs en ny mätning för att säkerställa att rummets RÖS-egenskap fortfarande är de förväntade. Även små förändringar i ett rum som att fel typ av kablar eller för många kablar dras genom en vågfälla kan påverka ett rums RÖS-egenskaper negativt.

Vid ändring av en lokal (t.ex. en ny kabelgenomföring) där dämpningsmätning tidigare har genomförts ska en förnyad analys eller mätning genomföras för att säkerställa

att krav på säkerhetsfunktionen skydd mot röjande signaler fortfarande uppfylls enligt bilaga 1 till [referens 14].

18.5.4 Kontrollerbart område

Ett annat alternativ till att använda utrustning i utrustningsklass och dämpade lokaler är att använda ett *kontrollerbart område* som dämpning. Då utnyttjar man luftens förmåga att dämpa de röjande elektromagnetiska signalerna och en kabels inbyggda impedans (det elektriska motståndet i en växelströmskrets) till att dämpa de ledningsbundna röjande signalerna. Kontrollerbart område används ofta som komplement till något av de andra två alternativen.

Då ett kontrollerbart område används som skydd är syftet med åtgärden att ingen obehörig ska kunna bedriva inhämtning av röjande signaler inom området eller göra påverkan på det befintliga skyddet mot röjande signaler. Detta uppnås med tillträdesbegränsning och bevakning av utrymmen, där utrustningen är placerad, samt av det kontrollerbara området.

18.5.5 Kontrollerbart område i internationella samarbeten

Om Försvarsmakten i ett internationellt samarbete använder alternativet kontrollerbart område för att uppnå ett tillräckligt RÖS-skydd för *hemliga uppgifter* måste det kontrollerade området bevakas genom en av Försvarsmakten tillhandahållen teknisk bevakning eller bevakas av svensk personal. Bevakningen ska stå under Försvarsmaktens kontroll.

Om Försvarsmakten i ett internationellt samarbete använder alternativet kontrollerbart område för att uppnå ett tillräckligt RÖS-skydd för att skydda *utrikesklassificerade uppgifter* som delges en annan stat eller mellanfolklig organisation bör kontroll av området upprätthållas av Sverige eller av en sådan stat eller mellanfolklig organisation som får ta del av uppgifterna.

18.5.6 Transport och förvaring av en RÖS-skyddad container

I insatsverksamheten används ofta RÖS-skyddade containrar som innehåller IT-system som är avsedda för behandling av hemliga och utrikesklassificerade uppgifter. För att man ska kunna lita på att RÖS-skyddet i en sådan container över tiden är intakt måste risken för att skyddet får skador p.g.a. slitage, transportskador och aktiv åverkan minimeras.

Vid transport och uppställning då en sådan container inte är i drift bör den tömmas på utrustning som, t.ex. IT-system, lagringsmedier och hemliga handlingar för att minska det totala skyddsvärdet. Dock bör man ändå hantera containern som skyddsvärd för att minimera risken att någon aktivt manipulerar RÖS-skyddet. Det innebär att en

sådan container bör stå på en bevakad plats som Försvarsmakten har kontroll över genom tillträdesbegränsning.

Om en sådan container inte kan stå på en bevakad plats som Försvarsmakten har kontroll över genom tillträdesbegränsning ska containern på nytt dämpningsmätas innan den tas i drift för att kontrollera att RÖS-skyddet fortfarande är intakt. Efter transport av en RÖS-skyddad container bör kontroll av att containern inte har några transportskador genomföras. Om en container har transportskador ska skadorna lagas. Containern ska därefter dämpningsmätas innan den tas i bruk för att kontrollera att RÖS-skyddet fortfarande är intakt.

Vid återkommande underhåll bör kontroll ske av t.ex. containerns uttagsfack, vågfällor, genomföringar och RÖS-skydd i dörr. Eventuella rostangrepp bör särskilt kontrolleras.

18.6 Skydd mot obehörig avlyssning

Skydd mot obehörig avlyssning är i IT-säkerhetssammanhang avsett att skydda mot aktörer som aktivt genomför teknisk inhämtning genom signalspaning mot en myndighets elektroniska kommunikationsnät som myndighetens IT-system är anslutna till. Syftet med säkerhetsfunktionen skydd mot obehörig avlyssning är att eliminera eller kraftigt begränsa effekten för en aktör som genomför en sådan signalspaning. Signalspaningen kan ske genom avlyssning av radiosignaler eller genom avlyssning av trådbunden kommunikation.

Grunder för skydd mot obehörig avlyssning av ett elektroniskt kommunikationsnät beskrivs i kapitel 10.

I vissa fall finns det inget mervärde i att använda kryptering för att skydda ett elektroniskt kommunikationsnät mot obehörig avlyssning (exempel 18:4).

Exempel 18:4

En kommunikationskabel förbinder två IT-system som står bredvid varandra i en datorhall. Till datorhallen har endast IT-tekniker som har behörighet att hantera båda IT-systemen tillträde. De personer som har tillgång till kommunikationskabeln har också tillgång till de IT-system som kommunicerar via kabeln, varför det inte finns något mervärde i att kryptera kommunikationen.

I många fall där man sätter upp ett elektroniskt kommunikationsnät inom en tillträdesbegränsad lokal kan skyddet mot obehörig avlyssning åstadkommas genom att

använda optisk fiberkabel eller skärmad kopparkabel som förläggs inspekterbar i hela sin sträckning. Kabeln kan också under korta sträckor förläggas i pansarrör där den inte går att förlägga inspekterbar, t.ex. i genomföringar.

Om en fiberkabel inte går att lägga inspekterbar i hela sin längd kan man förse fibern med avbrottslarm som varnar om fibern brutits vilket skulle kunna indikera att någon försöker manipulera kabeln. Larmet ska påkalla uppmärksamhet hos lämplig personal som kan avgöra vad larmet beror på och vidta nödvändig åtgärd. I vissa fall kan det vara aktuellt att larmet automatiskt stänger av trafiken i fiberkabeln till dess att kabeln bedöms som pålitlig och trafiken kan återupptas. Denna typ av larm kan ofta beskriva ungefär var på kabeln den har brustit genom att ange avståndet till avbrottet.

Användning av avbrottslarm på en fiberkabel måste följas upp med inspektioner där kontroll sker att ingen gjort åverkan på kabeln. Det är lämpligt att det i en IT-säkerhetsinstruktion för ett IT-system (avsnitt 14.8) eller i en IT-säkerhetsplan för en organisationsenhet (avsnitt 14.7) framgår rutiner för en sådan inspektion.

Säkerhetsfunktionen för skydd mot obehörig avlyssning ska inte förväxlas med skyddsåtgärder för att uppnå ett skydd mot obehörig avlyssning av en lokal eller ett område avsett för muntlig delgivning av hemliga uppgifter.

18.6.1 Godkänd säkerhetsfunktion för skydd mot obehörig avlyssning

> *Varje IT-system som är avsett för behandling av hemliga uppgifter skall vara försett med av myndigheten godkända säkerhetsfunktioner för skydd mot röjande signaler och obehörig avlyssning. Sådana säkerhetsfunktioner skall anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.*
>
> 7 kap. 13 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Se avsnitt 18.1 om en myndighets godkännande av säkerhetsfunktioner.

I Försvarsmakten gäller föreskriften även för IT-system som är avsedda för behandling av utrikesklassificerade uppgifter.[349]

349 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Med myndighet som enligt 7 kap. 13 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd ska godkänna säkerhetsfunktioner för skydd mot röjande signaler och obehörig avlyssning avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

9 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Se avsnitt 18.2 om MUST godkännande av säkerhetsfunktioner i Försvarsmakten.

18.7 Intrångsskydd

I detta kapitel avses med intrångsskydd: administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att skydda IT-system mot obehörig åtkomst från ett elektroniskt kommunikationsnät.

7 kap. 1 § 7 Försvarsmaktens föreskrifter om säkerhetsskydd

I dessa bestämmelser avses med elektroniskt kommunikationsnät: system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.

1 kap. 6 § 5 Försvarsmaktens interna bestämmelser om IT-säkerhet

Definitionen på elektroniskt kommunikationsnät är ursprungligen hämtad från 1 kap. 7 § lagen om elektronisk kommunikation. Föreskriften avser bl.a. telefoni, bildöverföring och kommunikation i ett IT-system och mellan IT-system. Avsikten är att definitionen ska vara heltäckande.

Att skydda ett IT-system mot obehörig åtkomst från ett elektroniskt kommunikationsnät avser att en angripare agerar genom ett elektroniskt kommunikationsnät. För åtkomsten behöver angriparen inte ha fysisk tillgång till IT-systemet. En angripare kan vara en obehörig men kan även vara en i övrigt behörig användare som från ett elektroniskt kommunikationsnät försöker ge sig större befogenheter i IT-systemet än han eller hon har behörighet till.

Ett elektroniskt kommunikationsnät kan vara ett nätverk som finns inom en myndighet men kan även vara ett externt nätverk som myndighetens IT-system är anslutna till.

Säkerhetsfunktionen intrångsskydd kan implementeras med teknikerna *filtrering*, *skydd av kommunikationsflöde* samt *härdning*. Vilken teknik som bör väljas beror på vilket slag av IT-system som ska skyddas och vilka gränsytor som IT-systemet har. Om IT-systemet är ett stort nätverk som innehåller flera delsystem kan det också finnas anledning att skydda inte bara externa gränsytor, utan även interna gränsytor inom IT-systemet för att få en bra funktion hos säkerhetsfunktionen intrångsskydd.

Skydd mot angrepp genom skadlig kod på ett lagringsmedium, t.ex. ett USB-minne, som används för att flytta uppgifter mellan två IT-system ska säkerhetsfunktionen skydd mot skadlig kod hantera.

18.7.1 Filtrering

Ett sätt att implementera säkerhetsfunktionen intrångsskydd är att låta inkommande och utgående informationsflöde passera genom någon form av filter som baserat på regler avgör om informationen ska få passera igenom filtret eller inte. Beroende på hur filtret implementeras kan intrångsskyddet variera i styrka.

Den vanligaste formen av intrångsskydd realiseras med en brandvägg eller datasluss i vilken man sätter upp regler för vilken trafik som får passera genom brandväggen. Då filter sätts upp för att reglera informationsflödet över en gränsyta måste man tänka på att filtret oftast inte kan ha samma konfiguration i båda riktningarna.

18.7.2 Skydd av kommunikationsflöde

En annan lösning för säkerhetsfunktionen intrångsskydd är att använda en kryptografisk metod som genom att dekryptera ett inkommande informationsflöde kan avgöra om dekrypteringen gått rätt till och därmed tillåta informationen att passera in i IT-systemet.

Det utgående informationsflödet krypteras på motsvarande sätt och för att kunna ta del av informationen måste sålunda den mottagande parten ha tillgång till rätt kryptonyckel. Denna metod säkerställer att det inkommande informationsflödet kommer från rätt avsändare, då ingen annan kan kryptera meddelanden utan att ha tillgång till rätt nyckel. För användning av krypto som intrångsskydd hänvisas till kravspecifikationer för signalskyddssystem i [referens 16].

18.7.3 Härdning

Med härdning avses att ett IT-systems exponerade tjänster minskas genom konfigurering. Syftet är att minska IT-systemets attackyta genom att minska antalet exponerade tjänster och därmed potentiella sårbarheter genom vilka IT-systemet kan attackeras.

Härdning innebär att tjänster som exponerar gränssnitt och som inte behövs för IT-systemets funktion stängs av. I ett stort IT-system med många delsystem kan viss typ av kommunikation styras till något delsystem och spärras i övriga delar.

En klientdator i ett IT-system kan även härdas genom att begränsa en användares rättigheter på klienten till sådana funktioner som endast användaren behöver. På så sätt minskas möjligheten för en person som har tillgång till klienten att använda klienten för intrång i andra delar av IT-systemet.

En effektiv härdning av ett IT-system underlättas av att IT-systemets huvudsakliga funktion inte är beroende av för många eller för komplicerade tjänster för att fungera.

I många IT-system kan en användare mata in uppgifter i ett skrivfält för att t.ex. logga in eller göra sökningar i en databas. Denna typ av skrivfält är också en gränsyta mot IT-systemet vars indata ska kontrolleras innan de avkodas av funktioner i IT-systemet. Annars finns risken att en användare kan skaffa sig ökade privilegier genom att få systemet att exekvera kommandon via skrivfältet.

18.7.4 Godkänd säkerhetsfunktion för intrångsskydd

> *Varje IT-system som är avsett för behandling av hemliga uppgifter skall vara försett med av myndigheten godkända säkerhetsfunktioner som skyddar mot intrång och som möjliggör intrångsdetektering. Sådana säkerhetsfunktioner skall anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.*
>
> 7 kap. 14 § första stycket Försvarsmaktens föreskrifter om säkerhetsskydd

Föreskriften gäller enbart för de IT-system som kommunicerar med ett eller flera andra IT-system.

Föreskriften möjliggör kommunikation mellan IT-system som hanterar information med olika informationssäkerhetsklasser och som då i praktiken kan ha olika krav på säkerhetsfunktionerna. Generellt ska varje IT-system svara för säkerheten över de egna gränssnitten men för t.ex. två delsystem som hanterar information i olika informationssäkerhetsklasser i samma IT-system kan man i vissa fall anse att det räcker att systemet med de högsta kraven på säkerhetsfunktionen ansvarar för säkerheten över gränsytan. I dessa fall ska säkerhetsfunktionen för intrångsskydd säkerställa att endast uppgifter som omfattas av högst den informationssäkerhetsklassen det lägre systemet är avsett att hantera får skickas dit. Det ska följaktligen inte vara möjligt att skicka uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/SECRET till ett IT-

system som är avsett att högst kunna hantera uppgifter som är placerade i informationssäkerhetsklassen HEMLIG/RESTRICTED.

Kraven på hur ett sådant filter ska vara beskaffat är höga. Om det finns behov av denna typ av informationsflöde mellan två system måste informationsflödet planeras noga i kravställningen på det delsystem som svarar för skyddet över gränsytan mellan systemen. Det är särskilt viktigt att det kommunikationsprotokoll som används över gränsytan finns väl beskrivet och lämpar sig för filtrering (se även avsnitt 13.10).

Se avsnitt 18.1 om en myndighets godkännande av säkerhetsfunktioner.

I Försvarsmakten gäller föreskriften även för IT-system som är avsedda för behandling av utrikesklassificerade uppgifter.[350]

> *Av 7 kap. 14 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd följer att varje IT-system som är avsett för behandling av hemliga uppgifter ska vara försett med en av myndigheten godkänd säkerhetsfunktion som skyddar mot intrång. Även övriga IT-system som är avsedda att användas av flera personer ska vara försedda med en sådan godkänd säkerhetsfunktion.*
>
> *Med myndighet enligt första stycket avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.*
>
> 10 kap. 1 § första och andra styckena Försvarsmaktens interna bestämmelser om IT-säkerhet

Även sådana IT-system som är avsedda för behandling av uppgifter som omfattas av sekretess enligt OSL men som inte rör rikets säkerhet samt sådana IT-system som inte är avsedda för behandling av uppgifter som omfattas av sekretess ska i Försvarsmakten vara försedda med en godkänd säkerhetsfunktion som skyddar mot intrång.

Föreskriften gäller enbart för sådana IT-system som ska användas av flera personer. Ett IT-system som ska användas av flera personer kan t.ex. vara en anställds bärbara dator som är avsedd att kopplas ihop med ett annat IT-system via ett elektroniskt kommunikationsnät. Föreskriften gäller inte för en anställds fristående dator som inte kommer att användas för kommunikation med andra IT-system och inte heller användas av någon annan än den ursprungliga användaren (s.k. enanvändarsystem).

Se avsnitt 18.2 om MUST godkännande av säkerhetsfunktioner i Försvarsmakten.

350 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

18.8 Intrångsdetektering

I detta kapitel avses med intrångsdetektering: administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att detektera intrång, eller försök till intrång eller förberedelse till intrång.

7 kap. 1 § 8 Försvarsmaktens föreskrifter om säkerhetsskydd

Syftet med säkerhetsfunktionen för intrångsdetektering är att övervaka de andra säkerhetsfunktionernas funktion och de öppna gränsytorna i det skyddade IT-systemet för att säkerställa att ingen utnyttjar eller försöker utnyttja sina egna eller någon annans behörigheter eller exponerade sårbarheter i IT-systemets gränsytor för att få åtkomst till det skyddade IT-systemet.

För att säkerhetsfunktionen för intrångsdetektering ska vara till någon nytta krävs det att säkerhetsfunktionen kan samla in sådan information som rör IT-systemets aktiviteter. Säkerhetsfunktionen måste även kunna analysera informationen för att slutligen rapportera resultatet av analyserna till en operatör som kan vidta åtgärder för att t.ex. förhindra ett pågående intrångsförsök.

I funktionen för intrångsdetektering övervakas de godkända informationsströmmarna inom IT-systemet och mot IT-systemets externa gränsytor för att detektera intrång eller försök till intrång.

Den enklaste form av intrångsdetektering kan bestå av en analys av säkerhetsloggen.

18.8.1 Godkänd säkerhetsfunktion för intrångsdetektering

Varje IT-system som är avsett för behandling av hemliga uppgifter skall vara försett med av myndigheten godkända säkerhetsfunktioner som skyddar mot intrång och som möjliggör intrångsdetektering. Sådana säkerhetsfunktioner skall anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

IT-system som är avsedda för behandling av uppgifter som har placerats i högst informationssäkerhetsklassen HEMLIG/RESTRICTED behöver dock inte förses med en säkerhetsfunktion som möjliggör intrångsdetektering.

7 kap. 14 § Försvarsmaktens föreskrifter om säkerhetsskydd

Föreskriften är enbart tillämplig på sådana IT-system som är avsedda för behandling av hemliga uppgifter av flera personer. Vidare gäller föreskriften enbart sådana IT-sys-

tem som är avsedda att kommunicera med andra IT-system. Om ett IT-system inte kommunicerar med något annat IT-system, s.k. enanvändarsystem, fyller intrångsskydd och intrångsdetektering ingen funktion.

Föreskriften möjliggör kommunikation mellan IT-system som hanterar information med olika informationssäkerhetsklasser (se även kommentar till föreskriften i avsnitt 18.7.4 om intrångsskydd).

Säkerhetsfunktionen för intrångsdetektering är ett mycket viktigt komplement till de andra säkerhetsfunktionerna. Den kan ses som en tilläggsfunktion till framförallt intrångsskydd och behörighetskontroll. I dessa två säkerhetsfunktioner måste en kompromiss mellan skyddet och funktionaliteten bestämmas och man måste lägga skyddet på en rimlig nivå. Vilken nivå ska en myndighet som omfattas av föreskriften besluta (se avsnitt 18.1 om en myndighets godkännande av säkerhetsfunktioner).

Det finns huvudsakligen två olika strategier för intrångsdetektering:

1. Analys av händelser i IT-systemet mot kända attackmönster eller signaturer av sådana händelser som kan tänkas få negativa följder för IT-systemet.
2. Analys av händelser i IT-systemet mot kända användningsprofiler i syfte att finna avvikelser mot det normala mönstret. Dessa användningsprofiler kan utvecklas för individer, för grupper av individer och andra objekt som t.ex. datorer.

Funktionen för intrångsdetektering ska erbjuda möjlighet att analysera intrång samt genera larm om missbruk av systemet görs. Detta kan t.ex. ske genom att loggar från relevanta system analyseras samt att en mekanism för att upptäcka intrång, ett s.k. intrångsdetekterande system (IDS) används. Beroende på vilken högsta informationssäkerhetsklass som de behandlade uppgifterna i systemet är placerade i, är det olika typer av mekanismer som kan vara aktuella att använda.

I Försvarsmakten gäller föreskriften även för IT-system som är avsedda för behandling av utrikesklassificerade uppgifter.[351]

351 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Av 7 kap. 14 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd följer att varje IT-system som är avsett för behandling av hemliga uppgifter ska vara försett med en av myndigheten godkänd säkerhetsfunktion som skyddar mot intrång. Även övriga IT-system som är avsedda att användas av flera personer ska vara försedda med en sådan godkänd säkerhetsfunktion.

Med myndighet enligt första stycket avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

Med myndighet som enligt 7 kap. 14 § Försvarsmaktens föreskrifter om säkerhetsskydd ska godkänna en säkerhetsfunktion som möjliggör intrångsdetektering avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

10 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Det finns inget krav på att ett IT-system som endast är avsett för behandling av sekretessklassificerade uppgifter eller ett IT-system som inte är avsett för behandling av uppgifter som omfattas av sekretess ska vara försedda med en godkänd säkerhetsfunktion för intrångsdetektering. Det kan dock i en säkerhetsmålsättning för sådana IT-system framkomma krav på ett sådant skydd. Ett exempel är om det i en säkerhetsanalys konstateras att IT-systemet exponeras mot ett nät, från vilket man bedömer intrångshotet som tillräckligt högt, för att en säkerhetsfunktion för intrångsdetektering ska vara en berättigad skyddsåtgärd.

Se avsnitt 18.2 om MUST godkännande av säkerhetsfunktioner i Försvarsmakten.

18.9 Skydd mot skadlig kod

I detta kapitel avses med skadlig kod: otillåten programkod som är till för att ändra, röja, förstöra eller avlyssna ett elektroniskt kommunikationsnät eller funktioner eller uppgifter i ett IT-system.

7 kap. 1 § 9 Försvarsmaktens föreskrifter om säkerhetsskydd

Skadlig kod är samlingsnamnet på det som vanligen kallas virus, maskar, trojaner och logiska bomber.

Skadlig kod kan i ett IT-system påverka IT-systemets egenskaper att upprätthålla det önskade skyddet avseende sekretess, riktighet, tillgänglighet och spårbarhet. Sekretessen åsidosätts t.ex. genom att en trojan öppnar en kanal ut ur systemet genom vilken den kopierar och sänder filer till en mottagare. Om kopieringen sker via en bakdörr i

IT-systemet utförs ingen loggning vilket medför att även spårbarheten påverkas. Riktigheten kan påverkas om den skadliga koden förändrar de uppgifter som behandlas i IT-systemet. Skadlig kod som förstör konfigurationer, hårdvara, eller som sprids i en sådan omfattning att de elektroniska kommunikationsnäten överbelastas, kan också påverka tillgängligheten negativt.

Skadlig kod kan spridas mellan datorer och mellan elektroniska kommunikationsnät på flera olika sätt. Spridning kan t.ex. ske via okontrollerade eller felaktiga anslutningar av bärbara datorer till elektroniska kommunikationsnät och e-post men även via flyttbara lagringsmedier som CD-skivor och USB-minnen. Spridningen underlättas ofta genom att den skadliga koden utnyttjar sårbarheter i IT-systemet. Datorer som är avsedda för uppkoppling mot Internet och som sedan kopplas in på, från Internet fristående elektroniska kommunikationsnät, har vid ett flertal tillfällen visat sig vara källan till spridning av skadlig kod.

En resursstark angripare kan skaffa sig förmåga att angripa IT-system som inte har fasta nätverksanslutningar utan som enbart kommunicerar med andra IT-system via flyttbara lagringsmedier som t.ex. USB-minnen. Ett USB-minne kan vara bärare av skadlig kod vars enda uppgift är att finna isolerade system och i det dolda lyfta ut information via USB-minnet till andra system där man via t.ex. e-post kan skicka den stulna informationen till angriparen.

Syftet med säkerhetsfunktionen för skadlig kod är att skydda en myndighets elektroniska kommunikationsnät och IT-system mot skadlig exekverbar programkod. Säkerhetsfunktionen skydd mot skadlig kod är beroende av ett effektivt intrångsskydd för att vara effektivt. Det är viktigt att IT-systemet kommunicerar över ett ändligt antal gränsytor så att säkerhetsfunktionen kan konfigureras att kontrollera samtliga inkommande dataflöden (t.ex. en fil) via dessa gränsytor.

Det finns i huvudsak tre sätt att skydda IT-system mot skadlig kod:

- Man kan förhindra skadlig kod från att komma in i IT-systemet.
- Man kan förhindra exekvering av skadlig kod.
- Man kan förhindra att skadlig kod sprids vidare till andra delar av systemet eller till andra system via det egna systemets gränsytor.

För att hindra skadlig kod från att komma in i ett IT-system är man beroende av ett väl fungerande intrångsskydd och ett system som är väl härdat (avsnitt 18.7.3). Detta för att begränsa IT-systemets attackyta och koncentrera inflödet av data till gränsytor där man kan kontrollera innehållet i flödet. Ett vanligt sätt är att använda antivirusprogram med *svartlistning* som metod för att avgöra om en fil får släppas in i IT-systemet. Svartlistning innebär att man identifierar skadlig kod utifrån en lista med signaturer på känd skadlig kod. En funktion i IT-systemet går igenom alla befintliga lagrade,

utgående och inkommande filer i jakt på dessa kända signaturer. Denna metod kräver att man kontinuerligt uppdaterar listan med kända signaturer på skadlig kod. Metoden fungerar ganska väl mot oriktade attacker men inte mot riktade attacker som ofta använder sig av modifierad eller specialskriven skadlig kod som är okänd och därför inte finns med i listan över känd skadlig kod.

Vitlistning innebär det omvända mot svartlistning, istället för att försöka identifiera den skadliga koden identifierar man istället de program och programkomponenter man vet är pålitliga. Alla program, programkomponenter, filer m.m. som inte kan identifieras som pålitliga hanteras automatiskt som okänd och därmed skadlig kod. En vitlista är därmed en förteckning över alla programpaket som är godkända att användas i ett IT-system. Denna metod fungerar väl mot riktade attacker men kräver en komplett förteckning över alla ingående komponenter i samtliga godkända programpaket. Vitlistning kan och bör även användas till att kräva en korrekt, komplett förteckning över alla i systemet använda skript, makron etc. Detta för att förhindra att skadlig kod göms i t.ex. Microsoft Office-dokument eller PDF-filer.

Observera dock att ibland används vitlistning i en mer generell bemärkelse där en förteckning över godkänd kod enbart görs utifrån en förteckning över tillverkare eller programnamn. Denna metod är dock riskabel då den oftast blir för generell samt förlitar sig på att tillverkare, programnamn m.m. har angivits korrekt i alla programkomponenter eller att en tillverkares kodsigneringscertifikat inte har använts för att signera en skadlig komponent.

För att förhindra att skadlig kod sprids vidare i ett IT-system eller till andra system bör man utföra samma eller andra motsvarande kontroller på flödet av data ut ur systemet. Här bör funktionen förstås också leta efter misstänkt programkod men här kan också trafikmönstret ge en indikation på om systemet är smittat av skadlig kod.

I ett IT-system som använder arbetsstationer eller datorer utan egna lagringsmedier kan säkerhetsfunktionen för skydd mot skadlig kod vara placerad centralt, t.ex. i en server i IT-systemet.

Det bör påpekas att säkerhetsfunktion för skydd mot skadlig kod inte nödvändigtvis behöver vara ett datorprogram. Skyddet kan även åstadkommas genom t.ex. *konfigurationsstyrning* samt styrning av vilka processer eller program som tillåts exekveras i en dator. Konfigurationsstyrning kan beskrivas som rutiner för att etablera, upprätthålla och förändra vilka mjuk- och hårdvaror som ska finnas i ett IT-system, hur de ska vara sammansatta i systemet och vilka inställningar som mjuk- och hårdvaror ska ha. Konfigurationsstyrning är en förutsättning för att kunna använda vitlistning. Även användningen av ett särskilt IT-system för kontroll av förekomst av skadlig kod på ett lagringsmedium kan vara en säkerhetsfunktion för skydd mot skadlig kod.

18.9.1 Godkänd säkerhetsfunktion för skydd mot skadlig kod

Varje IT-system som är avsett för behandling av hemliga uppgifter skall vara försett med en av myndigheten godkänd säkerhetsfunktion som skyddar mot skadlig kod. En sådan säkerhetsfunktion skall anpassas till den högsta informationssäkerhetsklass som någon av uppgifterna i IT-systemet har placerats i.

7 kap. 15 § Försvarsmaktens föreskrifter om säkerhetsskydd

Se avsnitt 18.1 om en myndighets godkännande av säkerhetsfunktioner.

I Försvarsmakten gäller föreskriften även för IT-system som är avsedda för behandling av utrikesklassificerade uppgifter.[352]

I 7 kap. 15 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd föreskrivs att varje IT-system som är avsett för behandling av hemliga uppgifter ska vara försett med en av myndigheten godkänd säkerhetsfunktion som skyddar mot skadlig kod. Även övriga IT-system ska vara försedda med en sådan godkänd säkerhetsfunktion.

Med myndighet enligt första stycket avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

10 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Om ett IT-system angrips av skadlig kod kan systemets skydd sättas ur funktion. Därför ska alla IT-system i Försvarsmakten förses med en godkänd säkerhetsfunktion som skyddar mot skadlig kod.

Föreskriften gäller för alla IT-system i Försvarsmakten oavsett vilka slag av uppgifter som IT-systemet är avsett att behandla, även i fråga om uppgifter som inte omfattas av sekretess enligt OSL. Föreskriften gäller även för sådana IT-system som endast ska användas av en person och som inte ska kommunicera med andra IT-system, s.k. enanvändarsystem.

Se avsnitt 18.2 om MUST godkännande av säkerhetsfunktioner i Försvarsmakten.

352 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

18.9.2 Förslag på förebyggande åtgärder

Nedan följer exempel på förebyggande åtgärder för att undvika skadlig kod:

- Uppdatera operativsystem och programvaror i det skyddade IT-systemet så snart som möjligt efter det att nya säkerhetsuppdateringar har blivit tillgängliga.
- Förse IT-system med antivirusprogram som utlöser larm för känd skadlig kod.
- Se till att det finns funktioner och rutiner för uppdatering av antivirusprogramvara.
- Använd antivirusprogramvara som kan kontrollera e-post.
- Viruskontrollera lagringsmedier, om det inte är uppenbart obehövligt, innan det används i Försvarsmaktens IT-system.
- Använd en särskild, inte nätverksansluten, dator för att kontrollera okända lagringsmedier.
- Använd endast auktoriserade program som kommer från kända och pålitliga leverantörer.
- Använd det lokala elektroniska kommunikationsnätets möjligheter för att se till att endast behöriga datorer kan kopplas in, t.ex. genom att använda MAC-adresslåsning.
- Kontrollera alla flyttbara lagringsmedier, t.ex. USB-minnen och andra lagringsmedier, med antivirusprogram. Kontrollera även programmets funktionalitet med samverkande program.
- Genomför regelbunden säkerhetskopiering.
- Registrera originalprogram. Skrivskydda det och säkerhetskopian.
- Reglera in- och utförsel av datorer och lagringsmedier till organisationsenheten, särskilt vid övningar.
- Reglera möjligheten att skriva och ändra i program.
- Testa nya program i en miljö som är skild från driftmiljön.

18.9.3 Användaransvar

En användare av ett IT-system kan genom att iaktta följande råd minska risken att skadlig kod införs i ett IT-system och uppmärksamma säkerhetsorganisationen på att skadlig kod förekommer.

- Använd endast lagringsmedier som är avsedda (godkända) för in- och utförsel av uppgifter. Vilka lagringsmedier som ska användas skiftar för olika IT-system.
- Anmäl om ett IT-system börjar bete sig misstänkt till helpdesk eller säkerhetsorganisationen.

- Anmäl e-post med konstiga bilagor till helpdesk eller säkerhetsorganisationen. Även om du inte öppnat dem. Det kan finnas fler som är drabbade och som inte varit lika uppmärksamma.

18.9.4 Åtgärder vid upptäckt av skadlig kod

Vid upptäckt av skadlig kod, eller vid misstanke om att skadlig kod finns, bör en användare av ett IT-system dokumentera följande.

1	*Stund*	Tidpunkten för upptäckten
2	*Ställe*	I vilken datormiljö den skadliga koden upptäcktes.
3	*Styrka*	Eventuell påverkan på IT-systemet.
4	*Slag*	Den skadliga kodens namn, om antivirusprogrammet meddelar det.
5	*Symbol*	Andra noteringar eller kännetecken.
6	*Sysselsättning*	Händelseförloppet i stort.
7	*Sedan*	Vidtagna åtgärder.
8	*Sagesman*	Vem som upptäckte den skadliga koden.

Om skadlig kod upptäcks i ett lagringsmedium som har skickats från någon annan bör avsändaren informeras snarast.

För IT-system som CIO är produktägare för bör en användare anmäla upptäckt av, eller misstanke om, skadlig kod, till servicedesk. Servicedesk ansvarar sedan för vidare rapportering.

Om skadlig kod hittas, eller misstänks finnas, ska detta i Försvarsmakten omedelbart rapporteras till närmaste chef, organisationsenhetens IT-säkerhetschef, insatsstaben i Högkvarteret samt till MUST.[353] CIO bör informeras i de fall han eller hon är produktägare för systemet. En driftägare behöver också informeras för att kunna vidta åtgärder i IT-systemet.

För ett IT-system som CIO inte är produktägare för, bör det i ackrediteringsunderlaget framgå hur upptäckt av, eller misstanke om, skadlig kod ska rapporteras. I utbildning av användare av sådana IT-system bör det framgå hur rapportering ska ske.

353 2 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet. Den operativa enheten i Högkvarteret finns inte längre men motsvaras av insatsstaben i Högkvarteret.

Vid borttagning av skadlig kod bör följande dokumenteras, som komplement till ovanstående:

1. Vem som tagit bort den skadliga koden.
2. Tidpunkten för borttagandet.
3. Misstänkt spridningsväg.
4. Vidtagna åtgärder.
5. När och till vilka rapportering har skett.

18.9.5 Kontroll av lagringsmedier i försändelser

Förslag till åtgärder för att förhindra att skadlig kod kommer in till, eller sprids från Försvarsmaktens IT-system:

- Ett lagringsmedium som skickas mellan organisationsenheter inom Försvarsmakten kontrolleras av avsändaren med avseende på skadlig kod. Mottagaren gör motsvarande kontroll innan det används. Hur kontrollen ska genomföras beror på hur säkerhetsfunktionen för skydd mot skadlig kod är utformad i IT-systemet.
- Till försändelsen bifogas en följesedel med anteckning om vem som har gjort kontroll avseende skadlig kod och med vilket program och programversion kontrollen gjorts.
- Regler för sändning och mottagande av lagringsmedier bör finnas i organisationsenhetens arbetsordning.
- I avtal med företag och överenskommelser med myndigheter som levererar information eller datorprogram måste det ingå en klausul som reglerar leverantörens skyldighet att genomföra kontroll med avseende på skadlig kod innan leverans görs till organisationsenheten.

19 Ackreditering av IT-system

I detta kapitel avses med ackreditering: ett sådant godkännande av ett IT-system från säkerhetssynpunkt som avses i 12 § tredje stycket säkerhetsskyddsförordningen (1996:633).

7 kap. 1 § 10 Försvarsmaktens föreskrifter om säkerhetsskydd

Systemet får inte tas i drift förrän det från säkerhetssynpunkt har godkänts av den för vars verksamhet systemet inrättas.

12 § tredje stycket säkerhetsskyddsförordningen

En myndighet som avser driftsätta ett IT-system som är avsett för behandling av hemliga uppgifter ska innan driftsättningen ha ackrediterat IT-systemet (godkänt systemet ur säkerhetssynpunkt). För att kunna ackreditera ett IT-system är det nödvändigt att myndigheten har säkerställt att det i och kring IT-systemet finns det säkerhetsskydd som behövs. Vilket säkerhetsskydd som behövs i och kring ett IT-system ges bl.a. av myndighetens säkerhetsanalys över vilka hot, risker och sårbarheter som kan påverka myndighetens säkerhetskänsliga verksamhet (se även avsnitt 14.4 om säkerhetsanalys). Om en myndighet inte kan uppnå eller upprätthålla erforderligt säkerhetsskydd för ett IT-system som är avsett för behandling av hemliga uppgifter måste myndigheten avstå från IT-systemet (se även avsnitt 13.1 om säkerhetsskydd i och kring IT-system).[354] I sådana fall får myndigheten inte fatta beslut om att IT-systemet är godkänt ur säkerhetssynpunkt och det kan därmed inte få driftsättas.

Föreskriften gäller endast för sådana IT-system som ska användas av flera personer.[355] I Försvarsmakten finns föreskrifter som innebär att även andra IT-system ska ackrediteras.

Beslut om ackreditering skall dokumenteras.

7 kap. 17 § Försvarsmaktens föreskrifter om säkerhetsskydd

När en myndighet ackrediterar ett IT-system ska beslutet naturligtvis dokumenteras. Anledningen till detta är bl.a. att det ska gå att spåra på vilka grunder ett IT-sys-

354 5 § första stycket säkerhetsskyddslagen.
355 Följer av 12 § andra stycket säkerhetsskyddsförordningen.

tem har ackrediterats. Ett beslut kan vara positivt (har godkänts) eller negativt (har inte godkänts). Även om en myndighet konstaterar att säkerhetsskyddet i och kring ett IT-system inte är tillräckligt kan myndigheten fatta ett beslut där det framgår att säkerhetsskyddet inte är tillräckligt och att IT-systemet därför inte får godkännas från säkerhetssynpunkt och inte får driftsättas.

I Försvarsmakten gäller föreskriften även för IT-system som är avsedda för behandling av utrikesklassificerade uppgifter.[356]

Ett IT-system som är avsett för behandling av utrikesklassificerade uppgifter får inte tas i drift förrän det har ackrediterats (godkänts från säkerhetssynpunkt) av den för vars verksamhet systemet inrättas.

2 kap. 8 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar

I Försvarsmakten ska även IT-system som är avsedda för behandling av utrikesklassificerade uppgifter godkännas ur säkerhetssynpunkt innan sådana IT-system driftsätts. Av föreskriften följer att även s.k. enanvändarsystem som är avsedda för behandling av utrikesklassificerade uppgifter ska ackrediteras.

I dessa bestämmelser avses med ackreditering: dels ett sådant godkännande av ett IT-system från säkerhetssynpunkt som avses i 12 § tredje stycket säkerhetsskyddsförordningen (1996:633), dels ett godkännande från säkerhetssynpunkt i övrigt av övriga IT-system.

1 kap. 6 § 12 Försvarsmaktens interna bestämmelser om IT-säkerhet

Begreppet *ackreditering* avser i Försvarsmakten även ett godkännande ur säkerhetssynpunkt för IT-system som inte är avsedda för behandling av hemliga uppgifter.

Ett IT-system som är avsett för behandling av hemliga uppgifter men som endast ska användas av en person får inte tas i drift förrän det har ackrediterats.

12 kap. 1 § andra stycket Försvarsmaktens interna bestämmelser om IT-säkerhet

356 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

I Försvarsmakten ska även ett enanvändarsystem som är avsett för behandling av hemliga eller utrikesklassificerade uppgifter ackrediteras (se även avsnitt 13.9 om sådana enanvändarsystem).[357] Alla IT-system i Försvarsmakten som är avsedda för behandling av hemliga eller utrikesklassificerade uppgifter ska således ackrediteras.

Ett IT-system som inte är avsett för behandling av hemliga uppgifter ska ackrediteras, om inte CIO eller den han bestämmer beslutar annat.

12 kap. 1 § tredje stycket Försvarsmaktens interna bestämmelser om IT-säkerhet

Föreskriften ger CIO, eller den han beslutar, mandatet att undanta ett IT-system som endast hanterar sekretessklassificerade uppgifter eller uppgifter som inte omfattas av sekretess från ackreditering. Föreskriften gäller inte för ett IT-system som är avsett att behandla utrikesklassificerade uppgifter.[358]

Beslut om ackreditering ska dokumenteras.

12 kap. 2 § Försvarsmaktens interna bestämmelser om IT-säkerhet

I Försvarsmakten ska även ackreditering av IT-system som inte är avsedda för behandling av hemliga uppgifter dokumenteras.

Ett ackrediteringsunderlag tas fram steg för steg inom ramen för auktorisationsprocessen. Därmed måste ett auktorisationsbeslut föregå ett eventuellt ackrediteringsbeslut.[359] Ett ackrediteringsunderlag utgörs av dokumentationen från utvecklingens olika faser. Underlaget måste vara så beskaffat att det finns en spårbarhet, från krav till vald lösning. Underlaget måste också vara utformat så att det är granskningsbart. Framtagningen av underlaget bör ske så, att verksamhetsansvariga involveras och därmed blir delaktiga varmed förutsättningar för att tillgodose verksamhetens krav skapas. En IT-säkerhetschef kan ha en stödjande och rådgivande roll, men han bör inte utses att genomföra arbetet.

Ackrediteringsunderlaget utgör en grund för en produktägares beslut om central ackreditering samt för en systemägares beslut om lokal ackreditering.

357 1 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
358 1 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
359 6 § Försvarsmaktens interna bestämmelser om IT-verksamhet.

19.1 Säkerhetsgranskning i och kring IT-system

Varje myndighet skall inför en ackreditering granska säkerheten i och kring ett IT-system och därvid särskilt beakta hur IT-systemet är avsett att samverka med andra IT-system. En sådan säkerhetsgranskning skall dokumenteras.

7 kap. 16 § Försvarsmaktens föreskrifter om säkerhetsskydd

Syftet med en säkerhetsgranskning är att säkerställa att det identifierade behovet av säkerhetsskyddsåtgärder är tillräckliga för att säkerhetsskyddet ska få avsedd effekt. En säkerhetsgranskning i och kring ett IT-system föregår alltid och ska ligga till grund för ett beslut om ackreditering.

Vid en säkerhetsgranskning är det särskilt viktigt att beakta hur ett IT-system samverkar med andra IT-system. Detta för att undvika att det i en kedja av IT-system kan finnas en svagaste länk som bidrar till att säkerheten i och kring de andra IT-systemen urholkas. Med ”kring ett IT-system” avses t.ex. tillträdesbegränsning i form av skalskydd och passagekontroll för lokaler och andra utrymmen för ett IT-system (se avsnitt 13.4 om tillträdesbegränsning kring ett IT-system).

Föreskriften gäller endast för IT-system som är avsett för behandling av hemliga uppgifter. I Försvarsmakten gäller föreskriften dock även för IT-system som är avsedda för behandling av utrikesklassificerade uppgifter.[360]

Produktägaren ska besluta i fråga om ackreditering av ett IT-system (central ackreditering). Produktägaren ska inför ett sådant beslut se till att säkerheten i och kring IT-systemet granskas.

Produktägaren ska se till att säkerheten granskas i och kring även sådana IT-system som inte ska ackrediteras, om inte CIO eller den han bestämmer beslutar annat.

Produktägaren ska se till att det vid säkerhetsgranskningen särskilt beaktas hur systemet är avsett att samverka med andra IT-system. En säkerhetsgranskning ska dokumenteras.

12 kap. 2 § Försvarsmaktens interna bestämmelser om IT-säkerhet

I Försvarsmakten är grundregeln att en säkerhetsgranskning av ett IT-system ska genomföras. Detta ska ske oberoende av vilka uppgifter som ska behandlas i systemet

360 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

och om det rör sig om en- eller fleranvändarsystem. CIO i Högkvarteret, eller den han bestämmer, får besluta att ett IT-system som inte ska ackrediteras inte heller behöver säkerhetsgranskas. Endast sådana IT-system som inte är avsedda för behandling av hemliga eller utrikesklassificerade uppgifter kan komma i fråga för ett sådant beslut av CIO.[361] [362] Om denna möjlighet ska användas beslutas inom ramen för auktorisation.[363]

19.2 MUST yttrande om säkerheten i ett IT-system

> *Innan ett IT-system som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer får ackrediteras centralt ska militära underrättelse- och säkerhetstjänsten i Högkvarteret yttra sig i fråga om säkerheten i systemet.*
>
> 12 kap. 4 § första stycket Försvarsmaktens interna bestämmelser om IT-säkerhet

Av föreskriftens första stycke följer att produktägaren inte får fatta beslut om ackreditering av ett IT-system som är avsett för behandling av hemliga uppgifter och som ska användas av flera personer förrän MUST har yttrat sig i fråga om säkerheten i systemet. Föreskriften gäller även för IT-system som är avsedda för behandling av utrikesklassificerade uppgifter.[364] Av första stycket följer även att MUST inte behöver yttra sig i fråga om säkerheten för sådana IT-system som är avsedda för behandling av hemliga eller utrikesklassificerade uppgifter men som endast ska användas av en person och som inte ska kommunicera med andra IT-system (s.k. enanvändarsystem).

I Försvarsmakten är det MUST som slutgiltigt i sitt yttrande om säkerheten i ett IT-system avgör om säkerhetsskyddet i och kring IT-systemet har uppnåtts och kan upprätthållas. En del av yttrandet är att avgöra om säkerhetsfunktionerna i ett IT-system är godkända (avsnitt 13.2). Ett yttrande ska även avgöra om de *tillkommande säkerhetskraven* (avsnitt 13.3) har uppfyllts.

Om MUST i ett yttrande om säkerheten i ett IT-system bedömer att säkerhetsskyddet *inte har uppnåtts* eller *inte kan upprätthållas* innebär det att säkerhetsskyddet inte har den utformning som krävs för säkerhetsskyddets syfte (bl.a. skydd mot spioneri, sabotage och andra brott som kan hota rikets säkerhet) och vad säkerhetsskyddet ska

361 12 kap. 3 § tredje stycket Försvarsmaktens interna bestämmelser om IT-säkerhet.
362 1 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet.
363 6 § Försvarsmaktens interna bestämmelser om IT-verksamhet.
364 1 kap. 3 § Försvarsmaktens interna bestämmelser om IT-säkerhet.

förebygga (bl.a. att hemliga uppgifter obehörigen röjs, ändras eller förstörs).[365] Då det i en verksamhet ska finnas det säkerhetsskydd som behövs kan ett sådant yttrande inte ligga till grund för att godkänna IT-systemet från säkerhetssynpunkt.[366] I sådana fall får Försvarsmakten inte fatta beslut om att IT-systemet är godkänt ur säkerhetssynpunkt och det kan därmed inte få driftsättas.[367]

> *Innan ett IT-system som inte är avsett för behandling av hemliga uppgifter får ackrediteras centralt ska militära underrättelse- och säkerhetstjänsten i Högkvarteret yttra sig i fråga om säkerheten i systemet, om inte CIO eller den han bestämmer beslutar annat.*
>
> 12 kap. 4 § andra stycket Försvarsmaktens interna bestämmelser om IT-säkerhet

Av föreskriftens andra stycke följer att produktägaren inte får fatta beslut om ackreditering av sådana IT-system som är avsedda för behandling av sekretessklassificerade uppgifter samt IT-system som inte är avsedda för behandling av uppgifter som omfattas av sekretess förrän MUST har yttrat sig i fråga om säkerheten i systemet. CIO i Högkvarteret, eller den han bestämmer, får besluta att MUST inte behöver avge något yttrande. Ett sådant beslut görs genom ett auktorisationsbeslut.[368] Föreskriftens andra stycke gäller både IT-system som används av flera personer och IT-system som endast används av en person.

Första och andra styckena i föreskriften innebär även att om MUST yttrande krävs inför en produktägares beslut i fråga om ackreditering av ett IT-system, så måste MUST avge ett yttrande som antingen är positivt eller negativt. MUST kan således inte avge ett yttrande som säger att ett yttrande inte kan avges.

19.3 Central ackreditering

> *Produktägaren ska besluta i fråga om ackreditering av ett IT-system (central ackreditering). Produktägaren ska inför ett sådant beslut se till att säkerheten i och kring IT-systemet granskas.*
>
> 12 kap. 2 § första stycket Försvarsmaktens interna bestämmelser om IT-säkerhet

365 6-7 §§ säkerhetsskyddslagen.
366 5 § första stycket säkerhetsskyddslagen.
367 12 § tredje stycket säkerhetsskyddsförordningen.
368 6 § Försvarsmaktens interna bestämmelser om IT-verksamhet.

Rollen produktägare beskrivs i avsnitt 2.2.2. Det är alltid en produktägare, som fattar beslut i fråga om ackreditering av ett IT-system i Försvarsmakten. Skrivningen ”i fråga om” innebär att produktägaren kan fatta antingen ett positivt eller ett negativt beslut om ackreditering.

Normalfallet är att produktägare finns vid Högkvarteret. För lokalt framtagna IT-system är det sannolikt så att produktägaren och systemägaren är samma person (chefen för en organisationsenhet). För ett sådant system kan chefen för en organisationsenhet i egenskap av produktägare och systemägare fatta centralt och lokalt ackrediteringsbeslut i samma beslut (se avsnitt 19.4 om lokal ackreditering).

Vid anskaffning av materiel genom FMV kan den av FMV levererade informationssäkerhetsdeklarationen (ISD) vara ett underlag för central ackreditering.[369]

19.4 Lokal ackreditering

Systemägaren ska besluta i fråga om ackreditering av ett IT-system som ska användas i den egna verksamheten (lokal ackreditering).

Innan ett IT-system får ackrediteras lokalt ska det ha ackrediterats centralt. Produktägaren ska se till att systemägaren förses med erforderligt underlag och erforderliga resurser för den lokala ackrediteringen.

Innan en systemägare beslutar om lokal ackreditering av ett IT-system som ska användas gemensamt inom en garnison, ska han ha inhämtat samråd från garnisonschefen.

12 kap. 5 § Försvarsmaktens interna bestämmelser om IT-säkerhet

I dessa bestämmelser avses med systemägare: den chef för en organisationsenhet som ansvarar för den del av ett IT-system som ska användas i den egna verksamheten.

1 kap. 6 § 14 Försvarsmaktens interna bestämmelser om IT-säkerhet

Endast en chef för en organisationsenhet kan vara systemägare. Se även avsnitt 2.2.3 om rollen chef för organisationsenhet.

Det är alltid chefen för den organisationsenhet som ansvarar för den del av ett IT-system som ska användas i den egna verksamheten som fattar beslut i fråga om lokal ack-

369 § A 9.5 Samordningsavtal mellan Försvarsmakten och Försvarets materielverk [referens 40].

reditering. För ett IT-system som används av flera systemägare ansvarar respektive systemägare för den del av IT-systemet som enbart är till för systemägarens verksamhet.

IT-system som inte ska ha någon systemägare (avsnitt 2.2.4) ska inte ackrediteras lokalt då godkännandet ur säkerhetssynpunkt har fattats genom beslut om central ackreditering. Behovet att lokalt ackreditera ett IT-system faller om chefen för organisationsenheten inte ansvarar för de delar av IT-systemet som ska användas i organisationsenhetens verksamhet.

En systemägaren får inte fatta beslut om lokal ackreditering förrän IT-systemet har ackrediterats av produktägaren. Systemägaren har nämligen inte tillräckligt underlag för att genomföra en lokal ackreditering förrän han eller hon har tagit del av det centrala ackrediteringsunderlaget. Således måste produktägaren bl.a. förse systemägaren med resurser som krävs för den lokala ackrediteringen. Sådana resurser kan t.ex. vara personal och ekonomi. Om systemägaren på något sätt ifrågasätter produktägarens underlag, får detta inte innebära att systemägaren vägrar att genomföra en lokal ackreditering. När den lokala ackrediteringen ska göras, bör systemägaren endast ta fasta på de lokala förhållandenas påverkan på IT-systemet. Detta innebär även att systemägare ska beakta eventuella villkor (central checklista för lokal ackreditering) för lokal driftsättning som produktägaren har ställt upp.

Om det vid den lokala ackrediteringen uppmärksammas att systemet som sådant är behäftat med brister – alltså förhållanden som produktägaren skulle ha uppmärksammat och dokumenterat – bör organisationsenheten dokumentera dessa iakttagelser och anmäla förhållandet till produktägaren. Om inte annat meddelas av produktägaren, eller en överordnad enhet, bör IT-systemet kunna tas i drift vid organisationsenheten i enlighet med vad som anges i den centrala ackrediteringen. Detta under förutsättning att IT-systemet dock har ackrediterats lokalt.

Garnisonssamordning avser bl.a. säkerhetstjänst.[370] En systemägare ska därför, innan han eller hon får fatta beslut om lokal ackreditering för ett IT-system som ska användas gemensamt inom en garnison, ha inhämtat samråd från garnisonschefen. Om garnisonschefen inte lämnar sitt samråd får inte systemägaren fatta beslut om lokal ackreditering.

Således bör innehållet i ett lokalt ackrediteringsunderlag utgå från det centrala ackrediteringsunderlaget samt centrala driftförutsättningar och hantera lokala förutsättningar för att beslut om lokal ackreditering ska kunna fattas.

370 Bilaga 2 till Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).

19.5 Omackreditering

Ett IT-system som är avsett för behandling av hemliga uppgifter och som har ackrediterats ska ackrediteras på nytt om det sker förändringar i eller kring systemet som kan påverka dess säkerhet.

Ett IT-system som inte är avsett för behandling av hemliga uppgifter och som har ackrediterats ska ackrediteras på nytt om det sker förändringar i eller kring systemet som kan påverka dess säkerhet, om inte CIO eller den han bestämmer beslutar annat.

IT-system som enligt beslut av CIO, eller den han har bestämt, inte har ackrediterats ska ackrediteras om det sker förändringar i eller kring systemet som kan påverka dess säkerhet, om inte CIO eller den han bestämmer beslutar annat.

12 kap. 6 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Första stycket i föreskriften gäller för IT-system som används både av flera personer och endast av en person. Förändringar i eller kring ett IT-system som kan påverka dess säkerhet kan t.ex. vara nya anslutningar till elektroniska kommunikationsnät, förändrad hotbild, signifikant utökad eller förändrad användarskara eller förändringar orsakade av nya verksamhetsbehov.

Beslut som fattas av CIO, eller den han bestämmer, enligt föreskriftens andra och tredje stycke, görs genom auktorisation.[371]

19.6 Framgångsfaktorer i ackrediteringsarbete

För att kunna besluta om att godkänna ett IT-system från säkerhetssynpunkt krävs ett antal förutsättningar. Särskilt kan bl.a. nämnas att det måste vara väldefinierat vilka krav som ska uppfyllas, vad som ska ackrediteras (IT-systemet med tillhörande gränsytor) samt vilka hot som är aktuella för IT-systemet att kunna möta och motstå.

Vilka krav som gäller för säkerhetsfunktioner i ett IT-system framgår av systemets IT-säkerhetsspecifikation (avsnitt 14.5). För Försvarsmakten har MUST beslutat krav på godkända säkerhetsfunktioner (KSF) [referenserna 7, 9 och 44].

371 6 § Försvarsmaktens interna bestämmelser om IT-verksamhet.

Ett centralt ackrediteringsbeslut bör från IT-säkerhetssynpunkt åtminstone innehålla följande.

- Bakgrund.
- Omfattning och avgränsningar.
- Ansvarsfördelning.
- Resultat från säkerhetsgranskning.
- MUST yttrande över säkerheten i systemet (i förekommande fall).
- Produktägarens bedömning mot bakgrund av säkerhetsgranskning och, i förekommande fall, MUST yttrande.
- Åtgärdslista.
- Beslut och giltighet.

Innehållet i en IT-säkerhetsspecifikation är av stor betydelse för bedömning av vilken IT-säkerhet som finns i ett IT-system. Krav på innehåll och form på en IT-säkerhetsspecifikation finns i MUST krav på godkända säkerhetsfunktioner (KSF) [referens 44].

Det lokala ackrediteringsunderlaget ska naturligtvis redovisa lokala förhållanden. Det är lämpligt att den lokala checklistan återfinns här och redovisas i åtgärdat skick.

Ett lokalt ackrediteringsbeslut bör från IT-säkerhetssynpunkt åtminstone innehålla följande.

- Bakgrund.
- Omfattning och avgränsningar.
- Ansvarsfördelning.
- Resultat från säkerhetsgranskning.
- MUST yttrande över säkerheten i systemet (i förekommande fall).
- Systemägarens bedömning mot bakgrund av produktägarens beslut om central ackreditering, säkerhetsgranskningen och, i förekommande fall, MUST yttrande.
- Åtgärdslista.
- Beslut och giltighet.

För att lyckas i ackrediteringsarbetet måste ansvariga för arbetet vara utsedda. Arbetet måste även vara förankrat i organisationen. Dessutom måste en stabsarbetsplan (projektplan) finnas där de ansvariga finns angivna och vilka resurser som de har till sitt förfogande samt när respektive del i stabsarbetsplanen ska vara avslutad. Vidare måste arbetet fortlöpande dokumenteras och rapporteras.

19.7 Samråd om register

Innan en myndighet inrättar ett register, som skall föras med hjälp av automatisk databehandling och som kan förutses komma att innehålla sådana uppgifter att utlämnandet av dem var för sig eller sammanställda kan skada totalförsvaret, skall myndigheten samråda med Försvarsmakten och, om uppgifternas natur ger anledning till det, Rikspolisstyrelsen. I fråga om uppgifter av betydelse för rikets säkerhet i övrigt skall i motsvarande fall samråd ske med Rikspolisstyrelsen.

12 § första stycket säkerhetsskyddsförordningen

Oavsett om säkerhetsskyddet vid en myndighet kontrolleras av Försvarsmakten eller Säkerhetspolisen är grunden att myndighetens samråd ska ske med Försvarsmakten om uppgifterna kan antas skada verksamhet som behövs för att förbereda Sverige för krig (totalförsvar).

En ansökan om samråd enligt 12 § säkerhetsskyddsförordningen sänds till säkerhetskontoret vid MUST varvid nedanstående punkter bör ingå.

- Myndighet och registeransvarig.
- På myndigheten ansvarig handläggare och dennes kontaktuppgifter.
- IT-systemets benämning.
- IT-systemets ändamål.
- IT-systemets informationsinnehåll (typ av uppgifter).
- Redovisning av sekretessbedömning av informationsinnehållet som avses behandlas i IT-systemet.
- Typ av IT-system som planeras användas; datortyp, koppling till nätverk, koppling för extern datakommunikation m.m.
- Systembeskrivning.
- En sammanfattning av vidtagna säkerhetsåtgärder för IT-systemet såsom t.ex.
  - behörighetskontroll,
  - säkerhetsloggning,
  - skydd mot röjande signaler,
  - skydd mot obehörig avlyssning (vilka eventuella kryptosystem som finns i IT-systemet),
  - intrångsskydd,

  – intrångsdetektering, och
  – skydd mot skadlig kod.
- Kvarstående åtgärder.
- Förvaltning, drift och underhåll (t.ex. säkerhetsuppdateringar).
- Kompletterande upplysningar beträffande registret, t.ex. om datautbyte med andra register och IT-system avses ske samt beskrivning på säkerhetslösningen kring sådana gränsytor.
- Myndighetens samlade bedömning över hur IT-systemet uppfyller säkerheten.

20 Kontroll

Generella grunder för kontroller beskrivs i H SÄK Grunder. MUST genomför tillsyn av säkerhetsskyddet vid Fortifikationsverket och Försvarshögskolan samt de myndigheter som hör till Försvarsdepartementet utom Kustbevakningen, Myndigheten för samhällsskydd och beredskap och Statens haverikommission.[372] [373] Tillsynen omfattar bl.a. informationssäkerheten för hemliga uppgifter.

Med tillsyn avses i Försvarsmakten en oberoende och självständig granskning av att en viss verksamhet uppfyller de krav och villkor som följer av lagar, förordningar, föreskrifter, eller andra villkor som meddelats i anslutning till dessa. Sådana villkor är även beslut om åtgärder som syftar till att vid behov åstadkomma rättelse vid utövande av verksamheten.[374]

I Försvarsmakten genomförs kontroller av den administrativa informationssäkerheten även för utrikesklasklassificerade uppgifter.[375] I IT-säkerhetskontroller inom Försvarsmakten kontrolleras även IT-säkerhet för utrikesklassificerade och sekretessklassificerade uppgifter samt IT-säkerhet för uppgifter som inte omfattas av sekretess enligt OSL.[376] Tabellen nedan sammanfattar för vilka slag av informationstillgångar som kontroll av administrativ informationssäkerhet respektive IT-säkerhet som genomförs inom Försvarsmakten.

	Hemliga uppgifter	Utrikesklassificerade uppgifter	Sekretessklassificerade uppgifter	Uppgifter som inte omfattas av sekretess
Administrativ informationssäkerhet	X	X		
IT-säkerhet	X	X	X	X

Vid tillsyn av informations- och IT-säkerhet vid en myndighet bedöms om en myndighet följer föreskrifterna i författningar om säkerhetsskydd. Vid tillsyn av informations- och IT-säkerhet vid en organisationsenhet bedöms om en organisationsenhet följer föreskrifterna i författningar om säkerhetsskydd samt de interna bestämmelser som gäller i Försvarsmakten om skyddet av andra slag av uppgifter. i tabellen nedan anger vilka författningar som bedömning ska genomföras mot.

372 39 § 1 säkerhetsskyddsförordningen.
373 6 kap. 2 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.
374 Bilaga 2 till Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).
375 2 kap. 1 § Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.
376 13 kap. 1-2 §§ Försvarsmaktens interna bestämmelser om IT-säkerhet

	Hemliga uppgifter		Utrikes-klassificerade uppgifter	Sekretess-klassificerade uppgifter	Uppgifter som inte omfattas av sekretess
	Myndighet	Organisationsenhet i Försvarsmakten			
Säkerhetsskyddslagen	x	x			
Säkerhetsskyddsförordningen	x	x			
Försvarsmaktens föreskrifter om säkerhetsskydd	x	x	x[377]		
Den kontrollerade myndighetens interna föreskrifter om säkerhetsskydd[378]	x				
Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel	Gäller inte	x	x[379]		
Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar	Gäller inte		x	[380]	
Försvarsmaktens interna bestämmelser om IT-säkerhet	Gäller inte	x	x	x	x

I tillsynen av en myndighet eller kontroll av säkerhetsskyddet vid en organisationsenhet ska även kontrolleras om säkerhetsskyddsnivån är anpassad till aktuellt säkerhetshot.[381] [382]

377 Med undantag av för vad som anges i 2 kap. 1 § 1 Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.
378 45 § Säkerhetsskyddsförordningen.
379 Med undantag av för vad som anges i 2 kap. 1 § 2 Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.
380 Krav på kontroll finns inte.
381 5 § säkerhetsskyddslagen.
382 6 kap. 1 § Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel.

20.1 Kontroll av administrativ informationssäkerhet

För att informationssäkerheten ska vara godkänd krävs att den kontrollerade har utformat informationssäkerheten så att den kontrollerade upprätthåller *kontroll över hemliga uppgifter*. Med kontroll över hemliga uppgifter avses här informationsklassificering, behörighet att få ta del av hemliga uppgifter och att ingen obehörig kan få ta del av uppgifterna då uppgifterna hanteras.

Brister som medför att kontrollen över hemliga uppgifter förloras, så att obehöriga kan få insyn i uppgifterna eller spårbarhet saknas i hanteringen av uppgifterna, är grund för ett underkänt säkerhetsskydd.

Om säkerhetsskyddet inte är tillräckligt för att förebygga att hemliga uppgifter *ändras* eller *förstörs* och skadorna bedöms äventyra rikets säkerhet är det grund för ett underkänt säkerhetsskydd, även om säkerhetsskyddsåtgärderna är tillräckliga för att förebygga ett obehörigt röjande av uppgifterna.

20.2 Kontroll av säkerhetsskåp

Säkerhetskontoret har gett ut riktlinjer för kontroll av enskilds säkerhetsskåp i Försvarsmakten [referens 21]. Av riktlinjerna framgår att ett säkerhetsskåps fysiska egenskaper och funktioner såsom rätt mått, skyddsnivå, lås, m.m. får kontrolleras.

Vid kontroll av innehållet i ett säkerhetsskåp får följande kontrolleras.

- Befintlighet av de hemliga handlingar som enligt kvittens vid expedition eller motsvarande har kvitterats av den enskilde (avsnitt 9.9),
- att hemliga handlingar förvaras åtskilda från övriga handlingar som inte innehåller hemliga uppgifter (avsnitt 9.11.3),
- att hemliga handlingar som är placerade i informationssäkerhetsklass HEMLIG/SECRET eller lägre förvaras åtskilda från hemliga handlingar som är placerade i informationssäkerhetsklassen HEMLIG/TOP SECRET (avsnitt 9.11.3).

Privata handlingar som förvaras i ett säkerhetsskåp får inte kontrolleras.

Vid misstanke om felaktig förvaring eller hantering av hemliga handlingar, exempelvis förekomst av svartkopior (avsnitt 9.17.1), får en kontroll av den enskildes säkerhetsskåp ske först efter beslut av chef för säkerhetsskyddskontroll alternativt enligt vad säkerhetskontoret bestämmer.

20.3 IT-säkerhetskontroll

En IT-säkerhetskontroll genomförs för att verifiera att de skyddsåtgärder som finns fyller sitt syfte och att de sårbarheter som accepterats, hanteras på ett säkert sätt. En IT-säkerhetskontroll måste även eftersträva att identifiera och medvetandegöra förbisedda brister i skyddet.

> *Kontroll av säkerheten i och kring ett IT-system som inte är avsett för behandling av hemliga uppgifter får endast genomföras med inriktningen att säkerställa att uppgifter i systemet*
>
> *- hanteras i enlighet med vad som föreskrivs i denna författning,*
>
> *- inte görs tillgängliga eller röjs för obehöriga,*
>
> *- är riktiga,*
>
> *- är spårbara, och*
>
> *- är tillgängliga för behöriga användare.*
>
> 13 kap. 5 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Kontroll av säkerheten i och kring ett IT-system som inte är avsett för behandling av hemliga eller utrikesklassificerade uppgifter får inte genomföras med någon annan inriktning än vad föreskriften anger (bild 20:1).

Med *i och kring* menas att det inte enbart är IT-systemet som ska kontrolleras utan även sådana förhållanden kring IT-systemet som kan påverka dess säkerhet. Som exempel kan nämnas sådan tillträdesbegränsning som skalskydd och inpasseringskontroll för lokaler och andra utrymmen där ett IT-system är placerat (avsnitt 13.4).

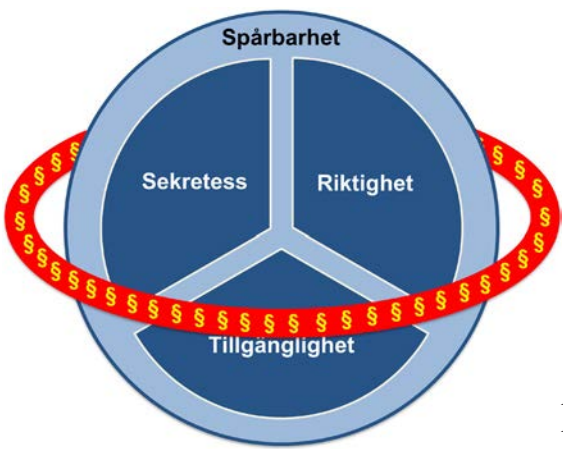


Bild 20:1 - Försvarsmaktens inriktning av IT-säkerhetskontroller inom myndigheten.

21 Avveckling

Inom ramen för Försvarsmaktens IT-livscykelmodell fattas beslut om avveckling. Detta innebär bl.a. att avveckling av ett IT-system ska föregås av auktorisation.

> *I dessa bestämmelser avses med ett IT-systems livscykel: tiden från och med det att ett IT-system börjar utvecklas till den tidpunkt när systemet har avvecklats.*
>
> 2 § 2 Försvarsmaktens interna bestämmelser om IT-verksamhet

> *Dessa bestämmelser gäller säkerheten i fråga om IT-system inom Försvarsmakten från och med den tidpunkt när ett sådant system börjar utvecklas till den tidpunkt när systemet har avvecklats (IT-systemets livscykel).*
>
> 1 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet

En produktägare som beslutar att avveckla ett IT-system ansvarar för att avvecklingen genomförs så att skyddet för uppgifterna upprätthålls under avvecklingen. Efter genomförd avveckling ska utrustning som innehåller hemliga uppgifter, t.ex. lagringsmedier, vara omhändertagna så att ett röjande av uppgifterna inte kan ske. Åtgärder för att uppnå detta kan vara att sådana lagringsmedier lämnas till expedition för arkivering, återanvändning eller förstöring.

Vid avslutning av en internationell militär insats hemställer produktägaren om auktorisation avseende avveckling. Därigenom kan bl.a. stöd ges, hur missionsspecifik information ska hanteras i samband med avveckling.

Inom ramen för materielprocessen fattas beslut om avveckling för de IT-system som är framtagna som materiel.[383] I sådan avveckling ska Försvarsmaktens krav på informationssäkerhet, inklusive IT-säkerhet, följas. Se avsnitt 2.4 om materielanskaffning.

CIO har beslutat en handledning för avveckling av IT-system [referens 47].

383 § A 2.3 Samordningsavtal mellan Försvarsmakten och Försvarets materielverk [referens 40].

21.1 Lagringsmedier i IT-system som avvecklas

Lagringsmedier som ingår i ett IT-system som avvecklas ska tas om hand så att kontrollen över dessa bibehålls, t.ex. vad gäller registrering (avsnitt 12.2.2). Förutsättningar för när lagringsmedier får återanvändas framgår i avsnitt 12.5 (hemliga uppgifter), avsnitt 12.6 (utrikesklassificerade uppgifter) samt avsnitt 12.7.2 (sekretessklassificerade uppgifter). Förutsättningar för hur lagringsmedier ska förstöras framgår i avsnitt 12.2.16 (hemliga uppgifter), avsnitt 12.6 (utrikesklassificerade uppgifter) samt avsnitt 12.7.4 (sekretessklassificerade uppgifter). Se även avsnitt 12.2.15 om Riksarkivets krav för bevarande av elektroniska handlingar.

Förhållandet att ett lagringsmedium som innehåller en hemlig eller utrikesklassificerad uppgift och som i samband med avveckling av ett IT-system inte kan återfinnas ska säkerhetsrapporteras (kapitel 22).

22 Rapportering

Rapportering vid röjande av uppgifter som omfattas av sekretess enligt OSL framgår i kapitel 11. Grunder för säkerhetsrapportering i Försvarsmakten framgår i H SÄK Grunder.

> *Sådana fel eller brister i säkerhetsskyddet som inte endast är av ringa betydelse skall snarast åtgärdas och anmälas till Försvarsmaktens högkvarter.*
>
> 1 kap. 8 § Försvarsmaktens föreskrifter om säkerhetsskydd

En myndighet har en skyldighet att anmäla fel eller brister i säkerhetsskyddet som inte endast är av ringa betydelse. En anmälan kan t.ex. avse fel och brister i hantering av hemliga handlingar eller kryptonycklar[384], hantering av lagringsmedier som avses innehålla eller som innehåller hemliga uppgifter eller IT-säkerhet för IT-system som är avsett för behandling av hemliga uppgifter.

Med Försvarsmaktens högkvarter avses MUST.

Även en organisationsenhet i Försvarsmakten omfattas av förskriften.

> *Anmälan som avses i 1 kap. 8 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd ska göras till Försvarsmaktens säkerhetsskyddschef.*
>
> *I 4 kap. 2 § Försvarsmaktens föreskrifter (FFS 1997:2) för Försvarsmaktens personal finns föreskrifter om skyldighet att rapportera säkerhetshotande verksamhet. Den som har tagit emot en sådan rapport ska vidarebefordra den till militära underrättelse- och säkerhetstjänsten i Högkvarteret.*
>
> 1 kap. 8 § Försvarsmaktens föreskrifter om säkerhetsskydd

Med Försvarsmaktens säkerhetsskyddschef avses chefen för MUST.[385]

384 25 § Försvarsmaktens föreskrifter om signalskyddstjänsten inom totalförsvaret.
385 11 kap. 5 § första stycket Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO).

Var och en som får kännedom om säkerhetshotande verksamhet eller misstänker sådan verksamhet skall snarast möjligt rapportera förhållandet till sin närmaste chef- arbetsledare eller till säkerhetschefen.

4 kap. 2 § Försvarsmaktens föreskrifter för Försvarsmaktens personal

Respektive underrättelse- och säkerhetsavdelning vid militärregionstaberna ska ta emot och hantera rapporter angående händelser som kan påverka informationssäkerheten för Försvarsmaktens informationstillgångar inklusive säkerheten i och kring Försvarsmaktens IT-system.

Rapportering ska göras snarast efter en inträffad händelse. Rapportering görs med hjälp av IS UNDSÄK enligt rutinen som finns beskriven i [referens 2]. Genom att rapportera säkerhetsrelaterade händelser i IS UNDSÄK möjliggörs att linjeorganisationen, på såväl taktisk, operativ som strategisk nivå samtidigt kan påbörja analys och vidta säkerhetshöjande åtgärder efter en sådan händelse. Om inte IS UNDSÄK finns tillgängligt där säkerhetsrapporten upprättas ska händelsen föras in i IS UNDSÄK av den nästkommande nivån där IS UNDSÄK finns tillgängligt.

Följande slag av händelser är exempel på när säkerhetsrapportering ska genomföras:

- Röjande av hemliga och utrikesklassificerade uppgifter som är placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre.
- Förlust (t.ex. genom stöld eller oaktsamhet) av ett lagringsmedium som innehåller hemliga, utrikes- eller sekretessklassificerade uppgifter.
- En förlust av en hemlig handling som är en allmän handling och som har placerats i informationssäkerhetsklass HEMLIG/CONFIDENTIAL eller högre.
- Ett lagringsmedium som innehåller en hemlig uppgift kan inte visas upp vid en inventering.
- Ett lagringsmedium som innehåller en hemlig uppgift kan inte återfinnas i samband med avveckling av ett IT-system.
- Signalskyddsincident (nyckel-, materiel- samt kort- eller certifikatsincident).

Kapitel 11 beskriver åtgärder vid förlust och röjande av uppgifter som omfattas av sekretess enligt OSL.

22.1 IT-säkerhetsrelaterad incident

Försvarsmakten blir alltmer beroende av informationsteknik i sin verksamhet samtidigt som hoten mot tekniken blir allt större. Då IT-systemen blir alltmer komplexa, blir de samtidigt mer sårbara och svårare att övervaka. Detta innebär att Försvarsmak-

ten måste prioritera sina insatser på säkerhetsområdet för att undvika IT-säkerhetsrelaterade incidenter. Samtidigt måste varje enskild rapportera IT-säkerhetsrelaterade incidenter som han eller hon upptäcker.

> *Händelser som kan påverka säkerheten i och kring Försvarsmaktens IT-system ska omedelbart rapporteras till närmaste chef, organisationsenhetens IT-säkerhetschef, operativa enheten i Högkvarteret samt till militära underrättelse- och säkerhetstjänsten i Högkvarteret.*
>
> 2 kap. 1 § Försvarsmaktens interna bestämmelser om IT-säkerhet

Med en IT-säkerhetsrelaterad incident avses i denna handbok *en händelse i eller kring ett IT-system där informationssäkerheten, d.v.s. sekretess, tillgänglighet, riktighet eller spårbarhet, har eller skulle kunna påverkas negativt*.

För att säkerställa att skyddet av våra informationstillgångar är tillräckligt är det viktigt att IT-säkerhetsrelaterade incidenter rapporteras. Information i rapporterna utgör, enskilt och sammanställt, underlag för förbättring av IT-säkerheten så att säkerheten i våra IT-system håller minst den nivå som beslutats vid ackrediteringen av IT-systemen.

Aktörer i Försvarsmakten som enligt IT-styrmodellen beställer, koordinerar och kontrollerar IT-tjänster bör orienteras om IT-säkerhetsrelaterade incidenter så att de med den kunskapen kan agera för förbättring av IT-säkerheten. Rapporter om IT-säkerhetsrelaterade incidenter är således inte endast en angelägenhet för den militära säkerhetstjänsten. De måste åtminstone i sammanställd form av säkerhetskontoret vid MUST delges till t.ex. CIO och produktionsledningen i Högkvarteret.

Att det finns krav på rapportering av IT-säkerhetsrelaterade incidenter hindrar inte driftägaren eller en IT-säkerhetschef att inom sina mandat genomföra åtgärder som syftar till att förbättra IT-säkerheten. En driftägare har också ett ansvar att säkerställa att IT-säkerheten upprätthålls. Detta ansvar utgår från krav i t.ex. ackrediteringsbeslut, beslut om driftförutsättningar och SLA. Det åligger också driftägaren att hantera, d.v.s. åtgärda fel och brister som uppstår vid en IT-säkerhetsrelaterad incident samt återställa systemets IT-säkerhet vid händelse av en sådan incident. Driftägaren, eller dennes representant, ska självfallet rapportera upptäckta incidenter.

Se även avsnitt 18.9.4 om åtgärder vid upptäckt av skadlig kod.

22.2 Försvarsmaktens Computer Emergency Response Team (FM CERT)

Försvarsmaktens Computer Emergency Response Team (FM CERT) är Försvarsmaktens resurs för hantering av IT-säkerhetsincidenter på strategisk och operativ nivå. FM CERT har huvuduppgifterna att:

- hantera IT-säkerhetsincidenter på strategisk och operativ nivå samt
- utarbeta en lägesbild som visar Försvarsmaktens IT-säkerhetsläge.

Uppgifterna löses genom att FM CERT har en samordnande roll i hantering av IT-säkerhetsincidenter och driver ärenden för att förbättra Försvarsmaktens förmåga att möta eller undvika IT-säkerhetsincidenter. Genom incidenthantering, egna utredningar och förbättringsarbete får FM CERT kännedom om säkerheten i Försvarsmaktens IT-system. De IT-säkerhetsrelaterade incidenter som säkerhetsrapporterats sammanställs och analyseras av FM CERT och är en del av Försvarsmaktens IT-säkerhetsläge.

FM CERT bedriver en kontinuerlig omvärldsbevakning av händelser och utveckling på IT-säkerhetsområdet. Genom att jämföra säkerheten och incidenter i Försvarsmakten med omvärlden drar FM CERT slutsatser om Försvarsmaktens IT-säkerhetsläge samt ger förslag på förbättringar. Lägesbilden redovisas i FM CERT:s årsrapporter och särskilda rapporter. Omvärldsbevakningen sammanfattas varje månad i FM CERT Nyhetsbevakning.

FM CERT kan även nås på e-post till *cert@mil.se* eller via telefon och fax. Observera dock att hemliga eller utrikesklassificerade uppgifter endast får skickas med ett godkänt signalskydd via e-post, telefon eller fax.

22.3 Anmälan till regeringen

> ***Om det vid utövandet av tillsynen över säkerhetsskyddet enligt 39 och 42 §§ konstateras brister som trots påpekanden inte rättas till, skall tillsynsmyndigheten anmäla förhållandet till regeringen. Detta gäller dock inte brister hos sådana enskilda som avses i 8 § första stycket säkerhetsskyddslagen (1996:627).***
>
> 48 § säkerhetsskyddsförordningen

Föreskriften innebär en skyldighet för Försvarsmakten att rapportera sådana brister, t.ex. vad gäller informationssäkerhet för hemliga uppgifter. Anmälningsskyldigheten gäller inte för företag som en myndighet har träffat ett säkerhetsskyddsavtal med.

23 Ikraftträdande- och övergångsbestämmelser

23.1 Försvarsmaktens föreskrifter om säkerhetsskydd

Har ett beslut om ackreditering fattats före ikraftträdandet av den nya författningen gäller inte föreskrifterna i 7 kap. 10, 11 och 13-15 §§ i den nya författningen.

Skall ett IT-system, på grund av förändringar som kan påverka säkerheten i det, på nytt ackrediteras enligt vad som följer av 12 § tredje stycket säkerhetsskyddsförordningen (1996:633) skall dock föreskrifterna i 7 kap. 10, 11 och 13-15 §§ i den nya författningen tillämpas.

Sjunde punkten i ikraftträdande- och övergångsbestämmelser
i Försvarsmaktens föreskrifter om säkerhetsskydd

Om ett IT-system är ackrediterat senast den 31 december 2003 behöver inte föreskrifterna om behörighetskontroll, säkerhetsloggning, röjande signaler, obehörig avlyssning, intrångsskydd, intrångsdetektering och skadlig kod tillämpas förrän vid den tidpunkt då IT-systemet ska ackrediteras på nytt. Se även avsnitt 19.5 om omackreditering.

Har ett underlag för ackreditering tagits fram före ikraftträdandet av den nya författningen gäller inte föreskrifterna i 7 kap. 10, 11 och 13-15 §§ i den nya författningen i fråga om detta underlag.

Åttonde punkten i ikraftträdande- och övergångsbestämmelser
i Försvarsmaktens föreskrifter om säkerhetsskydd

Med underlag avses det dokument som fastställer vilka hot som ställer krav på säkerhetsskydd och som sedan möts med säkerhetsmål. Inom Försvarsmakten benämns detta underlag säkerhetsmålsättning. Om ett sådant underlag har fastställts gäller inte föreskrifterna om behörighetskontroll, säkerhetsloggning, röjande signaler, obehörig avlyssning, intrångsskydd, intrångsdetektering och skadlig kod. De ska inte tillämpas förrän vid den tidpunkt då IT-systemet ska ackrediteras på nytt.

23.2 Försvarsmaktens interna bestämmelser om IT-säkerhet

Har ett beslut om ackreditering fattats före den 1 januari 2004 gäller inte föreskrifterna i 7 kap. 3 §, 8 kap. 1 §, 10 kap. 1 § och 11 kap. 1 § i den nya författningen.

Skall ett IT-system, på grund av förändringar som kan påverka säkerheten i det, på nytt ackrediteras skall dock föreskrifterna i 7 kap. 3 §, 8 kap. 1 § och 10 kap. 1 § och 11 kap. 1 § i den nya författningen tillämpas.

Tredje punkten i ikraftträdande- och övergångsbestämmelser i Försvarsmaktens interna bestämmelser om IT-säkerhet

Om ett IT-system är ackrediterat senast den 31 december 2003 behöver inte föreskrifterna om behörighetskontroll, säkerhetsloggning, intrångsskydd och skadlig kod tillämpas förrän vid den tidpunkt då IT-systemet ska ackrediteras på nytt. Se även avsnitt 19.5 om omackreditering.

Har ett underlag för ackreditering tagits fram före den 1 januari 2004 gäller inte föreskrifterna i 7 kap. 3 §, 8 kap. 1 §, 10 kap. 1 § och 11 kap. 1 § i den nya författningen i fråga om detta underlag.

Fjärde punkten i ikraftträdande- och övergångsbestämmelser i Försvarsmaktens interna bestämmelser om IT-säkerhet

Med underlag avses säkerhetsmålsättningen för det aktuella IT-systemet. Om ett sådant underlag har fastställts gäller inte föreskrifterna om behörighetskontroll, säkerhetsloggning, intrångsskydd och skadlig kod. De ska inte tillämpas förrän vid den tidpunkt då IT-systemet ska ackrediteras på nytt.

Bilaga 1 Översikt av författningar, handböcker m.m.

Tabellen visar vissa författningar som rör informationssäkerhet i Försvarsmakten och med anges vilka typer av uppgifter som författningarna gäller för.

Författning	Hemliga uppgifter	Utrikes-klassificerade uppgifter	Sekretess-klassificerade uppgifter	Uppgifter som inte omfattas av sekretess
Säkerhetsskyddslagen (1996:627)	X			
Säkerhetsskyddsförordningen (1996:633)	X			
Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhets-skydd	X			
Försvarsmaktens interna bestämmelser (FIB 2007:2) om säkerhetsskydd och skydd av viss materiel	X			
Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utri-kes- och sekretessklassificerade uppgifter och handlingar		X	X	
Försvarsmaktens interna bestämmelser (FIB 2009:1) om skade- och menbedömningar	X	X	X	
Försvarsmaktens interna bestämmelser (FIB 2007:5) om IT-verksamhet	X	X	X	X
Försvarsmaktens interna bestämmelser (FIB 2006:2) om IT-säkerhet	X	X	X	X

Följande förteckning visar vilka författningar, allmänna råd, handböcker, instruktioner och broschyrer som denna handbok hänvisar till.

Grundlagar
Tryckfrihetsförordningen (TF)
Yttrandefrihetsgrundlagen (YGL)

Lagar	Beteckning
Brottsbalken	
Lagen om anställningsskydd	1982:80
Förvaltningslagen	1986:223
Arkivlagen	1990:782
Lagen om undanförsel och förstöring	1992:1402
Lagen om totalförsvar och höjd beredskap	1992:1403
Säkerhetsskyddslagen	1996:627
Lagen om försvarsunderrättelseverksamhet	2000:130
Lagen om elektronisk kommunikation	2003:389
Offentlighets- och sekretesslagen (OSL)	2009:400
Lagen om upphandling på försvars- och säkerhetsområdet	2011:1029

Förordningar	Beteckning
Säkerhetsskyddsförordningen	1996:633
Förordning med bestämmelser för Försvarsmaktens personal	1996:927
Förordning med instruktion för Säkerhetspolisen	2002:1050
Förordningen om krisberedskap och höjd beredskap	2006:942
Förordning med instruktion för Försvarsmakten	2007:1266
Offentlighets- och sekretessförordningen (OSF)	2009:641
Förordningen om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet	2010:649

Föreskrifter	Beteckning
Riksarkivets föreskrifter om gallring av handlingar rörande hanteringen av hemliga och kvalificerat hemliga handlingar hos myndigheter under Försvarsdepartementet	RA-MS 2001:42[387]
Riksarkivets föreskrifter om gallring hos myndigheter under Försvarsdepartementet	RA-MS 2008:13
Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling)	RA-FS 2009:1
Riksarkivets föreskrifter och allmänna råd om tekniska krav för elektroniska handlingar (upptagningar för automatiserad behandling)	RA-FS 2009:2
Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet	MSBFS 2009:10
Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd	RPSFS 2010:3
Riksarkivets föreskrifter och allmänna råd om arkivlokaler	RA-FS 2013:4

Allmänna råd	Beteckning
Riksarkivets allmänna råd om registrering	RA-FS 1997:5

Försvarets författningssamling (FFS)	Beteckning
Försvarsmaktens föreskrifter för Försvarsmaktens personal	FFS 1997:2
Försvarsmaktens föreskrifter om säkerhetsskydd	FFS 2003:7
Försvarsmaktens föreskrifter om signalskyddstjänsten inom totalförsvaret	FFS 2005:2
Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar	FFS 2010:1
Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FM ArbO)	FFS 2013:4

Försvarsmaktens interna bestämmelser (FIB)	Beteckning
Försvarsmaktens interna bestämmelser om rätten att förhandla, ingå, ändra och säga upp internationella överenskommelser m.m.	FIB 2005:1
Försvarsmaktens interna bestämmelser om Försvarsmaktens personalansvarsnämnd	FIB 2005:4
Försvarsmaktens interna bestämmelser om IT-säkerhet	FIB 2006:2
Försvarsmaktens interna bestämmelser om säkerhetsskydd och skydd av viss materiel	FIB 2007:2
Försvarsmaktens interna bestämmelser om IT-verksamhet	FIB 2007:5
Försvarsmaktens interna bestämmelser om signalskyddstjänsten	FIB 2008:3
Försvarsmaktens interna bestämmelser om skade- och menbedömningar	FIB 2009:1

Handböcker, instruktioner och broschyrer			
Datum	Beteckning	Ärendemening	Anmärkning
2005		Instruktion totalförsvarets signalskyddstjänst, instruktion för hantering av aktiva kort, certifikat och korttermi-naler (I TST AKT), 2005	M7446-733103
2001-03-14	HKV 10 750:62687	Handbok Informationsteknik Hotbeskrivning (H SÄK IT Hot)	M7745-734051 Samskriven med Säkerhetspolisen.
2006-03-17	HKV 10 440:64709	Handbok för Försvarsmaktens säkerhetstjänst, Hotbedömning (H Säk Hot)	M7745-734022
2007-04-27	HKV 12 839:63626	Handbok totalförsvarets signalskyddstjänst, grundläggande regler för signalskyddstjänsten (H TST Grunder)	M7746-734002

Handböcker, instruktioner och broschyrer			
Datum	Beteckning	Ärendemening	Anmärkning
2007-08-31	HKV 10 440:70445	Handbok Säkerhetstjänst Säkerhets-skyddstjänst (H SÄK Skydd)	M7739-352005 Delar upp-hävda.
2009	MSB	Skydd mot brand - Före, under och efter räddningsinsats	Publikations-nummer: MSB 0109-09
2009	FMV	RÖS Röjande signaler – uppkomst, utbredning, skyddsmetoder, krav (BROSCHYR RÖS)	M7773-001851
2010-11-24	HKV 12 839:66443	Instruktion för användning av krypto för skyddsvärda uppgifter (I KSU) 2010	
2010-12-03	HKV 10 440:63815	Handbok Säkerhetsskyddad upphand-ling med säkerhetsskyddsavtal (Handbok SUA), 2010	M7739-352025
2011-01-14	HKV 10 440:50074	Handbok för Försvarsmaktens säker-hetstjänst, Sekretessbedömning Del A (H Säk Sekrbed A), 2011	M7739-352028
2012	Riksarkivet, Skrifter för offentlig förvalt-ning 2012:1	Redovisa verksamhetsinformation - Vägledning till Riksarkivets föreskrifter om arkivredovisning	ISBN 978-913832605-3
2013-04-29	HKV 10 440: 55631	Handbok för Försvarsmaktens Säkerhetstjänst Grunder (H SÄK Grunder), 2013	M7745-734011

Se även *Sammanställning över bestämmelser och riktlinjer för säkerhetstjänsten (SAM-SÄK)* som innehåller en förteckning över dokument som förekommer inom den militära säkerhetstjänstens arbetsområde, inklusive dokument om informationssäkerhet. Sammanställningen utges årligen av säkerhetskontoret vid MUST.

Bilaga 2 Referenser

I tabellen anges de skrivelser som handboken hänvisar till.

Referens	Dokument-datum	Beteckning	Ärendemening	Anmärkning
1	2001-04-20	HKV 10 750:63873	MUST uppfattning angående digitala kopiatorer	
2	2002-12-19	HKV 09 627:71169	Användarhandbok IS UNDSÄK-SÄK-rapportering	
3	2003-02-21	HKV 10 800:63110	Begäran om slutlig skadebe-dömning som inte är menbe-dömning	
4	2004-04-01	HKV KH 10 750:643	Riskanalys av säkerhetshoten mot Försvarsmaktens ledning-system	
5	2004-09-15	HKV H 10 750:81616	Hotbeskrivning av säkerhets-hoten mot Försvarsmaktens ledningssystem	
6	2004-10-29	HKV 20 400:75133	Beslut om regler för användning av Försvarsmaktens IT-system	
7	2004-12-20	HKV 10 750:78976	Beslut om krav på godkända säkerhetsfunktioner, ver. 2.0	Benämns KSF 2.0.
8	2005-02-04	HKV 20 400:62526	Riktlinjer för de användare av Försvarsmaktens IT-system som inte omfattas av Beslut om reg-ler för användning av Försvars-maktens IT-system (HKV 2004-10-29 20 400:75133)	
9	2005-02-22	HKV H/C 10 750:80237	Beslut om krav på godkända säkerhetsfunktioner, version 2.0	Benämns KSF 2.0.
10	2005-04-05	HKV 10 700:65482	Beslut om Försvarsmaktens informationssäkerhetspolicy	Återgiven i bilaga 4.
11	2005-04-08	HKV 20 400:66602	Översättning till engelska av riktlinjer för vissa användare av Försvarsmaktens IT-system	
12	2006-01-31	HKV 10 700:61686	Översättning till engelska av Försvarsmaktens informations-säkerhetspolicy	
13	2006-02-06	HKV 20 400:62414	Rättsliga och arkivvårdsmässiga aspekter på hantering av skräppost, s.k. spam, inom Försvarsmakten	

Referens	Dokument-datum	Beteckning	Ärendemening	Anmärkning
14	2006-03-24	HKV 10 755:65114	Beslut om krav på skydd mot röjande signaler (RÖS)	
15	2007-02-19	HKV 20 400:63221	Kryptering av känsliga person-uppgifter	
16	2007-03-27	HKV 12 830:65517	Krav för signalskyddssystem avsedda för Totalförsvaret	
17	2007-06-08	HKV 09 884:69593	Revidering av tillämpningsbe-slut avseende gallring av hand-lingar av tillfällig eller ringa betydelse	
18	2007-07-02	HKV 10 753:60387	Direktiv för Försvarsmakten angående förstöring av digitala lagringsmedier	
19	2008-05-15	HKV 09 884:68744	Gallring av sekretessbevis	
20	2008-05-23	HKV 12 830:70698	Användning av Svenskt krypto för att skydda EU-klassade uppgifter	
21	2008-06-26	HKV 10 700:72561	Riktlinjer vid kontroll av enskilds säkerhetsskåp	
22	2008-11-19	HKV 09 600:78555	Reglering av lagring av privata filer på FM lagringsytor	
23	2009-02-11	HKV H/S 10 750:80501	Fördjupning av hot- och sårbar-hetsanalys av Försvarsmaktens IT-system	
24	2009-06-26	HKV 10 812:60437	Direktiv om utformning av sekretessmarkering i Försvars-makten	
25	2010-06-07	SÄPO AD400-6353-10	Vägledning vid anmälan om brott mot BrB 19 kap	
26	2010-06-23	HKV 10 700:60542	Direktiv angående sektionering m.m. i utrymmen för IT och tele-kommunikation	
27	2010-06-30	HKV H/S 10 817:81235	Beslut om handläggning av ärenden rörande menbedöm-ningar vid FMTM	
28	2010-06-30	HKV H/R 10 817:81236	Beslut om handläggning av ärenden rörande menbedöm-ningar vid HKV INSS SFL	
29	2010-06-30	HKV H/R 10 817:81237	Beslut om handläggning av ärenden rörande menbedöm-ningar vid MUST	

Referens	Dokument-datum	Beteckning	Ärendemening	Anmärkning
30	2010-07-09	HKV 10 800:59981	Informationsblad om säkerhet och sociala nätverk	
31	2010-11-01	HKV 12 830:65753	Godkännande och användning av svenskt krypto för att nationellt skydda NATO-klassade uppgifter	
32	2011-02-11	HKV 10 800:53077	Beslut avseende informationsfoldrar Säkerhet och sociala medier samt Säkerhet och mobiltelefoner	
33	2011-02-25	HKV 10 700:53939	Brister i säkerhetskuvert	
34	2011-03-31	HKV 12 839:54833	Direktiv för förstöring av CD-skiva som innehåller eller har innehållit kryptonycklar	
35	2011-06-15	Diarienummer 10-8756	Robust elektronisk kommunikation - vägledning för användare vid anskaffning	Rapportnummer PTS-ER-2011:16
36	2011-09-09	HKV 17 100:63719	Försvarsmaktens riktlinjer för sociala medier	
37	2011-10-31	HKV 09 100:64970	Fastställande av Försvarsmaktens IT-styrmodell	
38	2011-12-05	HKV 09 626:68847	CIO instruktion för spamhantering i Försvarsmakten	
39	2012-02-14	HKV 10 750:52359	IT Säkerhetsgodkännande för Överskrivningsverktyg 2.1	
40	2008-12-09	HKV 03 200:76010	SAMO FM – FMV 2009	Benämns samordningsavtal mellan Försvarsmakten och Försvarets materielverk.
	2012-12-19	HKV 03 200:69018	Missiv överenskommelse FM FMV	
41	2012-02-23	HKV 10 800:52919	Innebörd av begreppet ”Mission Secret”	
42	2012-03-16	HKV 10 700:50011	Instruktion avseende kunskapskrav säkerhetstjänst	
43	2012-08-24	HKV 09 621:60961	Auktorisationsbeslut B1-B4 avseende Mobila externa lagringsenheter med USB och Firewire	

Referens	Dokument-datum	Beteckning	Ärendemening	Anmärkning
44	2012-09-24	HKV 10 750:64354	Beslut om krav på godkända säkerhetsfunktioner version 3.0 (KSF v3.0)	Benämns KSF 3.0.
45	2012-09-25	HKV 01 800:28148	Natos säkerhetsbestämmelser	Från UD.
46	2012-12-13	HKV 10 700:66098	Beslut avseende kravuppfyllnad vid förstöring av optiska lagringsmedier av typen CD, DVD och Blu-ray med INTIMUS 005S	
47	2012-12-14	HKV 09 621:69249	Fastställande av handledning för avveckling av IT-system	
48	2013-11-11	FM2013-2582:1	Beslut om handläggning av ärenden rörande menbedömningar	
49	1990-12-27	Överbefälhavaren USL 903:64258	Gemensamt nyttjande av hemliga handlingar	Ska inte längre tillämpas.
50	1991-02-15	Chefen för flygvapnet 903:60394	Gemensamt nyttjande av hemliga handlingar	Ska inte längre tillämpas.
51	1992-11-13	Upplands flygflottilj DET BÅLSTA 903:2232	Säkerhetsskyddsföreskrifter för BUSH	Ska inte längre tillämpas.

Se även *Sammanställning över bestämmelser och riktlinjer för säkerhetstjänsten (SAMSÄK)* som innehåller en förteckning över dokument som förekommer inom den militära säkerhetstjänstens arbetsområde, inklusive dokument om informationssäkerhet. Sammanställningen utges årligen av säkerhetskontoret vid MUST.

Bilaga 3 Blanketter

Tabellen visar blanketter i Försvarsmakten som rör informationssäkerhet. Blanketterna är tillgängliga i elektroniskt format i blankettbanken i Försvarsmaktens intranät.

Benämning	M-nummer
Beslut - Gemensam användning av hemliga handlingar samt samförvaring	M7102-122780E
Bilaga - Gemensam användning av hemliga handlingar	M7102-122790E
Förlustanmälan - Hemliga handlingar	M7102-500420E
Secrecy declaration	M7102-660335E
Sekretessbevis	M7102-660330E

Bilaga 4 Försvarsmaktens informationssäkerhetspolicy

Det övergripande målet med Försvarsmaktens informationssäkerhet är att säkerställa ett tillräckligt skydd för myndighetens informationstillgångar såväl inom som utom landet, så att rätt information är tillgänglig för rätt person i rätt tid på ett spårbart sätt.

Information är en av Försvarsmaktens viktigaste tillgångar och utgör en förutsättning för att kunna bedriva verksamheten. Våra informationstillgångar måste därför behandlas och skyddas på ett tillfredsställande sätt mot de risker som förekommer. Lagar och förordningar utgör grunden för Försvarsmakten i detta arbete, dessutom ska ingångna överenskommelser och avtal följas.

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationssäkerheten omfattar Försvarsmaktens informationstillgångar utan undantag.

Med informationssäkerhet avses i Försvarsmakten:

- att informationen finns tillgänglig när den behövs,
- att informationen är och förblir riktig,
- att informationen endast är tillgänglig för dem som är behöriga att ta del av och använda den, samt
- att hanteringen av informationen är spårbar.

Försvarsmaktens definition på informationssäkerhet innebär alltså ett vidare begrepp än det som anges i säkerhetsskyddslagen.

Informationssäkerhet är en integrerad del av Försvarsmaktens verksamhet.

Alla som i någon utsträckning hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är samtidigt ett ansvar för chefer på alla nivåer inom Försvarsmakten att aktivt verka för att alla ska inse informationssäkerhetens betydelse. Vidare ska cheferna verka för att en positiv attityd till säkerhetsarbetet genomsyrar all verksamhet. Försvarsmaktens informationssäkerhetsarbete leds och samordnas av militära underrättelse- och säkerhetstjänsten i Högkvarteret. Var och en i Försvarsmakten ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgångar.

Informationssäkerhetspolicyn förverkligas genom att vi uppnår våra mål, följer våra handlingsplaner och genomför de åtgärder som beskrivs i Försvarsmaktens regelverk.

Varje organisationsenhet är bunden av denna policy, vilket medför att det inte finns något utrymme att besluta om lokala policies som avviker från denna informationssäkerhetspolicy.

Den som använder Försvarsmaktens informationstillgångar på ett sätt som strider mot denna informationssäkerhetspolicy kan bli föremål för åtgärder från myndighetens sida.

Militära underrättelse- och säkerhetstjänsten i Högkvarteret ansvarar för att informationssäkerhetspolicyn årligen granskas och vid behov revideras.

Denna informationssäkerhetspolicy är fastställd av överbefälhavaren den 5 april 2005 och ska börja tillämpas den 1 maj 2005.

Bilaga 5 Begreppsförklaringar

Alla begrepp som används i handboken beskrivs inte här. Grundläggande begrepp för den militära säkerhetstjänstens organisation och verksamhet som inte direkt hör till informationssäkerhetsområdet är inte medtagna.

Begrepp eller förkortning	Betydelse
Ackreditering	Dels ett sådant godkännande av ett IT-system från säkerhetssynpunkt som avses i 12 § tredje stycket säkerhetsskyddsförordningen, dels ett godkännande från säkerhetssynpunkt i övrigt av övriga IT-system.
Aggregation	Förhållandet att den sammantagna konsekvensen av att flera uppgifter röjs överstiger konsekvensen för en enskild uppgift. Se avsnitt 4.3.4 i H Säk Sekrbed A.
Aktörsdrivet hot	En mänsklig aktörs möjligheter att medvetet förorsaka en oönskad händelse med negativa konsekvenser (H SÄK Grunder).
Allmän handling	En handling är allmän om den förvaras hos en myndighet och antingen är inkommen till myndigheten eller upprättad hos myndigheten (2 kap. 3 § TF).
Arbetshandling	En handling som inte är en allmän handling.
Autentisering	Se avsnitt 18.3.2.
Behandling	Avser i denna handbok varje åtgärd eller serie av åtgärder som vidtas för en uppgift, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring. Avsikten är att begreppet ska vara heltäckande. Begreppet är i detta avseende hämtat från 3 § personuppgiftslagen.
Behörighetskontroll	Administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att kontrollera en användares identitet, styra en användares behörighet att använda IT-systemet och dess resurser samt registrera användaren.
Bilateralt säkerhetsskyddsavtal	En mellanstatlig och för Sverige bindande överenskommelse om hur hemliga uppgifter ska utbytas, hanteras och skyddas i relation till den andra staten.

Begrepp eller förkortning	Betydelse
Caveat	En anteckning som innebär begränsningar i att delge eller använda handlingar. Benämns i internationella sammanhang caveat. Benämningen kan även användas i andra områden än informationssäkerhet och har då andra betydelser.
CERT	Computer Emergency Response Team.
CIO	Chief information officer.
Elektroniskt kommunikationsnät	System för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.
Enanvändarsystem	Ett IT-system som administreras och används av endast en person. Systemet får inte vara anslutet mot något elektroniskt kommunikationsnät för att få kallas enanvändarsystem.
Gallring	Förstöring av allmänna handlingar eller uppgifter samt överföring till annan databärare om överföringen leder till informationsförlust, förlust av möjliga informationssammanställningar, förlust av sökmöjligheter eller förlust av möjligheter att fastställa informationens autenticitet.
Gallringsfrist	Den tid som ska förflyta innan gallringsbara handlingar ska gallras ut.
Gemensam användning	Se avsnitt 9.15.1.
Hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten (SIS HB 550 Utgåva 3). Indelas i aktörsdrivet respektive icke aktörsdrivet hot (H SÄK Grunder).
Hotbild	Uppsättning hot som bedöms föreligga mot en viss verksamhet (SIS HB 550 Utgåva 3).
Härdning	Se avsnitt 18.7.3.
Icke aktörsdrivet hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten, vilken ej är förorsakad av en mänsklig aktörs avsiktliga gärningar (H SÄK Grunder). Generellt kan icke aktörsdrivna hot indelas i tre kategorier: Naturliga fenomen (t.ex. naturkatastrofer, sjukdomar). Fel i tekniska system (t.ex. buggar, materialfel). Icke uppsåtliga mänskliga gärningar (t.ex. slarv, olyckor).
Informationsförlust	Händelse där kontrollen över en informationstillgång förloras med risk för att informationstillgången röjs, t.ex. genom att en handling tappas bort eller ofullständigt förstörs.

Begrepp eller förkortning	Betydelse
Informationssäkerhet	Med informationssäkerhet avses i Försvarsmakten att informationen finns tillgänglig när den behövs, att informationen är och förblir riktig, att informationen endast är tillgänglig för dem som är behöriga att ta del av och använda den, samt att hanteringen av informationen är spårbar (Försvarsmaktens informationssäkerhetspolicy).
Informationssäkerhetsklass	Informationssäkerhetsklasserna är en indelning av säkerhetsskyddet i Försvarsmakten, samt i de myndigheter för vilka Försvarsmakten har föreskriftsrätt över.
Informationstillgång	En organisations informationsrelaterade tillgångar (SIS HB 550 Utgåva 3).
Intrångsdetektering	Administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att detektera intrång, eller försök till intrång eller förberedelse till intrång
Intrångsskydd	Administrativa eller tekniska åtgärder, eller både administrativa och tekniska åtgärder, som vidtas för att skydda IT-system mot obehörig åtkomst från ett elektroniskt kommunikationsnät.
IT-system	System med teknik som hanterar och utbyter information med omgivningen.
IT-säkerhet	Åtgärder som syftar till att uppnå och vidmakthålla den nivå av säkerhet som bl.a. lagar, förordningar, Försvarsmaktens författningar, Försvarsmaktens informationssäkerhetspolicy, särskilda skrivelser och verksamhetens behov ställer på ett IT-system.
IT-säkerhetsplan	Se avsnitt 14.7.
IT-säkerhetsrelaterad incident	En händelse i eller kring ett IT-system där informationssäkerheten, d.v.s. sekretess, tillgänglighet, riktighet eller spårbarhet, har eller skulle kunna påverkas negativt.
IT-säkerhetsspecifikation (ITSS)	Specificerar vilka IT-säkerhetsförmågor systemet ska ha, och på vilket sätt och i vilken miljö systemet ska användas för att systemet ska anses vara tillräckligt säkert samt hur systemets säkerhetsfunktioner och driftmiljö samverkar för att säkerställa dessa säkerhetsegenskaper.
Konfigurationsstyrning	Rutiner för att etablera, upprätthålla och förändra vilka mjuk- och hårdvaror som ska finnas i ett IT-system, hur de ska vara sammansatta i systemet och vilka inställningar som mjuk- och hårdvaror ska ha.

Begrepp eller förkortning	Betydelse
Konsekvens	Resultat av en händelse med negativ inverkan (SIS HB 550 Utgåva 3). I en säkerhetsanalys behandlas främst utfallet av oönskade händelser, dvs. händelser med en eller flera konsekvenser som är negativa för verksamheten. Konsekvensen skall i en säkerhetsanalys ses som en bedömning av värdet eller kostnaden av den skada som uppstår i en skyddsvärd tillgång om en oönskad händelse inträffar till följd av ett visst hot.
Kontinuitetsplan	Plan över vilka åtgärder som ska vidtas vid avbrott eller störningar i IT-systemets funktion.
Kontrollerbart område	Se avsnitt 18.5.4.
Krypto för skyddsvärda uppgifter (KSU)	Se avsnitt 10.3.
Kvalificerat hemlig uppgift	Uppgift som omfattas av sekretess enligt OSL och som är av synnerlig betydelse för rikets säkerhet.
Känsliga personuppgifter	Personuppgifter som avslöjar en persons ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv.
Lagringsmedium	Permanent minnesmedium som används för att kunna lagra och läsa uppgifter.
LIMITE	Se avsnitt 9.1.6.
Meddelarfrihet	Regler i TF som innebär att alla har rätt att, med vissa begränsningar, fritt meddela uppgifter och underrättelser i vilket ämne som helst för publicering i tryckta och enligt 1 kap. 5 § TF därmed jämställda skrifter. För radio m.m. gäller motsvarande regler i YGL.
Medförande	Se avsnitt 9.13.
Mellankvittering	Se avsnitt 9.9.2.
MUST	Militära underrättelse- och säkerhetstjänsten.
Regelverksanalys	Beskriver vilka lagar, förordningar, föreskrifter, interna bestämmelser och andra regler som är aktuella för ett IT-system och för de uppgifter som avses behandlas i IT-systemet. Benämndes tidigare författningsanalys.
Rikets säkerhet	Sägs innebära den yttre säkerheten för vårt nationella oberoende och den inre säkerheten för skydd av vårt demokratiska statsskick (sidan 22, prop. 1995/96:129).

Begrepp eller förkortning	Betydelse
Risk	Risker uttrycks ofta i termer av en kombination av en händelses konsekvenser (inklusive ändrade omständigheter) och därtill relaterad sannolikhet för förekomst (ISO/IEC Guide 73:2009). I en säkerhetsanalys innebär risk en systematisk sammanvägning av förväntad sannolikhet för och konsekvens av att en oönskad händelse inträffar till följd av ett visst hot, kopplat till en definierad verksamhet, en specifik skyddsvärd tillgång och en specifik konsekvensskala. En bedömd risk uttrycks i en av fem risknivåer.
Riskhantering	Samordnade aktiviteter för att styra och kontrollera en organisation med avseende på risk (ISO/IEC Guide 73:2002).
Riskhanteringsbeslut	Medvetna (dokumenterade) chefsbeslut om hur chefen ställer sig till analyserade risker i förhållande till värdet av sökta effekter eller uppgiftens lösande och kostnader för riskminskning. (FM Riskhanteringsmodell 2009).
Röjande signaler	Inte önskvärda elektromagnetiska eller akustiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs.
RÖS	Röjande signaler.
Samförvaring	Se avsnitt 9.12.
SAMSÄK	Sammanställning över bestämmelser och riktlinjer för säkerhetstjänsten. Innehåller en förteckning över dokument som förekommer inom den militära säkerhetstjänstens arbetsområde, inklusive dokument om informationssäkerhet. Sammanställningen utges årligen av säkerhetskontoret vid MUST.
Sekretessbevis	Se avsnitt 8.1.
Sekretessklassificerad uppgift	Se avsnitt 6.3.
Sekretessmarkering	Märkning på en allmän handling om att den bedöms innehålla någon uppgift som omfattas av sekretess enligt OSL.
Signalkontroll	Kontroll av signalskyddet i telekommunikations- och IT-system i syfte att klarlägga dels riskerna för obehörig åtkomst eller störande eller manipulering av data, dels att systemen används enligt gällande regler, samt kontroll av röjande signaler (RÖS).
Skadlig kod	Otillåten programkod som är till för att ändra, röja, förstöra eller avlyssna ett elektroniskt kommunikationsnät eller funktioner eller uppgifter i ett IT-system.
Skalskyddsklass	Se avsnitt 18.5.3.

Begrepp eller förkortning	Betydelse
Skyddsåtgärd	Handling, procedur eller tekniskt arrangemang som, genom att minska sårbarheten möter identifierat hot (SIS HB 550 Utgåva 3). Med skyddsåtgärd avses i detta sammanhang även sådana skyddsåtgärder som vidtas med avseende på säkerhetsskyddskrav, dvs. säkerhetsskyddsåtgärder. Vidare avses också åtgärder som minskar en risk genom att undvika den, överföra den eller som reducerar identifierade hot.
SLA	Service Level Agreement. En överenskommelse om servicenivå.
Svartkopia	Oregistrerade kopior av eller utdrag ur hemliga eller utrikesklassificerade handlingar som ska registreras.
Svartlistning	Se avsnitt 18.9.
Sårbarhet	Brist i skyddet av en tillgång exponerad för hot (SIS HB 550 Utgåva 3).
Säkerhetsanalys	Tillämpningen av begreppet säkerhetsanalys inom ramen för bedrivande av militär säkerhetstjänst avser såväl identifiering och prioritering av skyddsvärda tillgångar, bedömning av säkerhetshot, sårbarheter och risker som prioritering och hantering av risker inklusive beslut om skyddsåtgärder. Begreppet säkerhetsanalys är i detta avseende att jämföra med begrepp som riskanalys eller risk management.
Säkerhetsfunktion	En eller flera funktioner i ett IT-system som upprätthåller säkerheten enligt regler om hur uppgifter i IT-systemet ska skyddas.
Säkerhetsklarering	Se avsnitt 7.9.
Säkerhetslogg	Behandlingshistorik över händelser som är av betydelse för säkerheten i eller kring ett IT-system.
Säkerhetsloggning	Manuell eller automatisk registrering, eller både manuell och automatisk registrering, av händelser som är av betydelse för säkerheten i eller kring ett IT-system.
Säkerhetsmålsättning	Dokumenterade analyser av vilket skydd som ett IT-system kräver och vilka åtgärder som måste vidtas för att skyddet ska få avsedd effekt.
TEMPEST	Vanlig benämning hos andra stater som motsvarar *röjande signaler*.
Tillgång	Allt som är av värde för organisationen (SIS HB 550 Utgåva 3).
Tillträdesbegränsning	Den del av säkerhetsskyddet som ska förebygga att obehöriga får tillträde till platser där de kan få tillgång till hemliga uppgifter eller där verksamhet som har betydelse för rikets säkerhet bedrivs.

Begrepp eller förkortning	Betydelse
Tillträdesskydd	Skyddsåtgärder som ska förebygga att obehöriga får tillträde till platser där de kan få tillgång till utrikesklassificerade eller sekretessklassificerade uppgifter.
UNCLASSIFIED	Se avsnitt 9.1.5.
Underkvittering	Se avsnitt 9.9.1
Upptagning	Se avsnitt 12.2.
Utrikesklassificerad uppgift	Se avsnitt 6.2.
Utrustningsklass	Se avsnitt 18.5.2.
Verksamhetsanalys	Beskriver i IT-säkerhetssammanhang den verksamhet som ett IT-system är tänkt att stödja, vilka slag av uppgifter som IT-systemet är avsett att behandla samt verksamhetens krav på skydd.
Verkställighetsföreskrifter	Föreskrifter av rent administrativ karaktär för tillämpningen av en lag och i viss mån också föreskrifter som fyller ut en lag materiellt men utan att tillföra den något väsentligt nytt.
Vitlistning	Se avsnitt 18.9.
Åtkomstkontroll	Se avsnitt 18.3.5.
Ägarföreträdare	Roll som används för materiel. Har inför regeringen ansvar för förnödenheternas status, sekretess, befintlighet och redovisning.
Ägarföreträdarens representant	Roll som används för att hantera materiel. Ansvarar för att representera ägarföreträdaren bl.a. vad gäller drift- och ekonomistyrning, uppföljning och analys, konfigurationsläge, modifieringar, tekniskt systemstöd och teknisk utveckling.

Deltagare

Kim Hakkarainen (redaktör och ämnesexpert)

Zenobia Rosander (projektledare och ämnesexpert)

Ann-Marie Löf (ämnesexpert)

Stefan Styrenius (ämnesexpert)

FÖRSVARSMAKTEN

107 85 STOCKHOLM. Tel 08-788 75 00, Fax 08-788 77 78.
www.forsvarsmakten.se

Handbok Säkerhetstjänst
Informationssäkerhet
M7739-352056