FÖRSVARSMAKTENS INTERNA BESTÄMMELSER

FIB 2010:2
Utkom från
trycket 2010-01-21
Omtryck

Föreskrifter om ändring i Försvarsmaktens interna bestämmelser (FIB 2006:2) om IT-säkerhet;

beslutade den 15 januari 2010.

Försvarsmakten föreskriver i fråga om Försvarsmaktens interna bestämmelser (FIB 2006:2) om IT-säkerhet

dels att i 1 kap. 5, 9 §§, 2-4 kap., 5 kap. 1 §, 6-11 kap., 12 kap. 1–4 §§ samt 13 kap. 2 och 3 §§ ordet ”skall” ska bytas ut mot ”ska”,

dels att nuvarande 3-14 kap. ska betecknas 4-15 kap,

dels att 1 kap. 3, 6 och 7 §§ samt 15 kap. 1 § ska ha följande lydelse,

dels att det i föreskrifterna ska införas ett nytt kapitel, 3 kap. av följande lydelse,

dels att punkterna 3 och 4 i ikraftträdande- och övergångsbestämmelserna ska ha följande lydelse.

Författningen kommer därför att ha följande lydelse från och med den dag då denna författning träder i kraft.

1 kap. Inledande bestämmelser

Grunder

1 § 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).

2 § Med hemlig handling och hemlig uppgift avses i dessa bestämmelser detsamma som i 4 § säkerhetsskyddsförordningen (1996:633).

3 § Dessa bestämmelser gäller IT-system som är avsedda för behandling av såväl hemliga uppgifter, utrikesklassificerade uppgifter, sekretessklassificerade uppgifter som övriga uppgifter, om inget annat anges i denna författning. Det som anges för hemliga uppgifter ska också gälla för utrikesklassificerade uppgifter. *(FIB 2010:2)*

4 § Vad som i Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd föreskrivs för myndighet eller chef för myndighet avser inom Försvarsmakten dess organisationsenheter respektive cheferna för organisationsenheterna, om inget annat anges i denna författning.

5 § I 5 § säkerhetsskyddsförordningen (1996:633) finns föreskrifter om säkerhetsanalys. Vad som där föreskrivs om sådan analys samt dokumentation ska fullgöras av varje organisationsenhet. *(FIB 2010:2)*

Definitioner

6 §[1] I dessa bestämmelser avses med

1. *IT-system:* system med teknik som hanterar och utbyter information med omgivningen,

2. *utrikesklassificerad uppgift:* en uppgift som av en utländsk myndighet eller mellanfolklig organisation har klassificerats i någon av nivåerna TOP SECRET, SECRET, CONFIDENTIAL eller RESTRICTED eller motsvarande och som är sekretessbelagd enligt 15 kap. 1 § offentlighets- och sekretesslagen (2009:400) men som inte rör rikets säkerhet,

3. *sekretessklassificerad uppgift:* En uppgift som är sekretessbelagd enligt offentlighets- och sekretesslagen men som inte rör rikets säkerhet och som inte är en utrikesklassificerad uppgift,

4. *sekretessklassificerad handling:* En handling som innehåller sekretessklassificerad uppgift,

5. *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,

6. *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,

7. *säkerhetsfunktion:* en eller flera funktioner i ett IT-system som upprätthåller säkerheten enligt regler om hur uppgifter i IT-systemet ska skyddas,

8. *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,

[1] Senaste lydelse FIB 2007:4.

9. *säkerhetslogg:* behandlingshistorik över händelser som är av betydelse för säkerheten i eller kring ett IT-system,

10. *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,

11. *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,

12. *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,

13. *produktägare:* den som är utsedd att vara produktägare enligt 4 § Försvarsmaktens interna bestämmelser (FIB 2007:5) om IT-verksamhet, och

14. *systemägare:* den chef för en organisationsenhet som ansvarar för den del av ett IT-system som ska användas i den egna verksamheten. *(FIB 2010:2)*

7 §[2] I Försvarsmaktens interna bestämmelser (FIB 2007:5) om IT-verksamhet finns bestämmelser om auktorisation. *(FIB 2010:2)*

8 § har upphävts genom *(FIB 2007:4)*.

Planer

9 § Varje organisationsenhet ska i en plan ange vilka åtgärder som ska vidtas vid avbrott eller störningar i IT-systemets funktion. *(FIB 2010:2)*

10 § Chefen för en organisationsenhet ska i en skriftlig plan (IT-säkerhetsplan) fastställa riktlinjer för IT-säkerheten inom organisationsenheten. *(FIB 2010:2)*

[2] Senaste lydelse FIB 2007:4.

IT-säkerhetschef, biträdande IT-säkerhetschef och IT-säkerhetsansvarig

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

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.

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. *(FIB 2010:2)*

2 kap. Rapportering

1 § 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. *(FIB 2010:2)*

3 kap. Hantering av lagringsmedium för sekretessklassificerade uppgifter

1 § 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. *(FIB 2010:2)*

2 § 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. *(FIB 2010:2)*

3 § 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. *(FIB 2010:2)*

4 kap. Utveckling, anskaffning, användning och avveckling

1 § 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.

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. *(FIB 2010:2)*

2 § 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. *(FIB 2010:2)*

3 § Analyser som avses i 1 och 2 §§ i detta kapitel ska dokumenteras i säkerhetsmålsättningar. *(FIB 2010:2)*

4 § 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. *(FIB 2010:2)*

5 § 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. *(FIB 2010:2)*

5 kap. Elektronisk kommunikation

1 § 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. *(FIB 2010:2)*

6 kap. Utbildning

1 § Chefen för en organisationsenhet ska, innan en person tilldelas behörighet att använda ett IT-system, se till att han eller hon på ett säkert sätt kan hantera systemet. Användaren ska ha genomgått erforderlig utbildning i IT-säkerhet med godkänt resultat. Organisationsenheten ska föra en förteckning över vilka som har genomgått en sådan utbildning i IT-säkerhet. *(FIB 2010:2)*

2 § 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.

7 kap. Behörighetskontroll m.m.

1 § 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. *(FIB 2010:2)*

2 § 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. *(FIB 2010:2)*

3 § 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. *(FIB 2010:2)*

8 kap. Säkerhetsloggning

1 § 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. *(FIB 2010:2)*

2 § 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. *(FIB 2010:2)*

3 § Produktägaren ska se till att säkerhetsloggen kan analyseras och att loggen har erforderlig detaljeringsgrad. *(FIB 2010:2)*

4 § Systemägaren eller den han bestämmer ska se till att säkerhetsloggar analyseras. *(FIB 2010:2)*

5 § Chefen för organisationsenheten ska se till att användare av ett IT-system informeras om att säkerhetsloggning sker. *(FIB 2010:2)*

6 § Varje säkerhetslogg vid organisationsenheten ska förvaras i läsbar form. Den ska fortlöpande kopieras och vårdas. *(FIB 2010:2)*

9 kap. Skydd mot röjande signaler och obehörig avlyssning

1 § 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. *(FIB 2010:2)*

10 kap. Intrångsskydd och intrångsdetektering

1 § 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. *(FIB 2010:2)*

11 kap. Skydd mot skadlig kod

1 § 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. *(FIB 2010:2)*

12 kap. Ackreditering m.m.

1 § Av 12 § tredje stycket säkerhetsskyddsförordningen (1996:633) följer att ett IT-system som är avsett för behandling av hemliga uppgifter och som ska användas av flera personer inte får tas i drift förrän det har ackrediterats av den för vars verksamhet systemet inrättas.

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.

Ett IT-system som inte är avsett för behandling av hemliga uppgifter ska ackrediteras, om inte CIO eller den han bestämmer beslutar annat. *(FIB 2010:2)*

2 § Beslut om ackreditering ska dokumenteras. *(FIB 2010:2)*

3 § 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. *(FIB 2010:2)*

4 § 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.

Innan ett IT-system som inte är avsett för behandling av hemliga uppgifter får ackrediteras centralt ska militära underrättelse- och säkerhetstjänsten i Hög- kvarteret yttra sig i fråga om säkerheten i systemet, om inte CIO eller den han bestämmer beslutar annat. *(FIB 2010:2)*

5 § 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. *(FIB 2010:2)*

6 § 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. *(FIB 2010:2)*

13 kap. Kontroll

1 § I 6 kap. Försvarsmaktens interna bestämelser (FIB 2007:2) om säkerhetskydd och skydd av viss materiel finns föreskrifter om var militära underrättelse- och säkerhetstjänsten i Högkvarteret ska genomföra säkerhetsskyddskontroller. *(FIB 2010:2)*

2 § 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. *(FIB 2010:2)*

3 § Chefen för en organisationsenhet ska genomföra kontroller av säkerheten i och kring sådana IT-system inom enheten som inte är avsedda för behandling av hemliga uppgifter.

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. *(FIB 2010:2)*

4 § Kontroller som avses i 2 och 3 §§ i detta kapitel ska dokumenteras. *(FIB 2010:2)*

5 § 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.

14 kap. Internationell verksamhet

1 § Bestämmelserna i detta kapitel gäller

1. för utlandsstyrkan inom Försvarsmakten,

2. när Försvarsmakten deltar i internationell fredsfrämjande verksamhet eller inom ramen för internationellt samarbete eller i utbildning eller förberedelser för sådan verksamhet, och

3. när Försvarsmakten utomlands deltar i förevisningar av materiel eller verksamhet.

2 §[3] Chef för kontingent får för utlandsstyrkan, i fråga om verksamhet utanför Sverige, fatta beslut som avviker från 7 kap. Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd samt denna författning, om det är oundgängligen nödvändigt för verksamheten. I fråga om verksamhet som avses i 1 § 2 och 3 i detta kapitel och som genomförs utanför Sverige gäller detsamma chef för organisationsenhet eller, om beslut i sådan ordning inte kan fattas, av chef för kontingent.

Beslut som avses i första stycket ska dokumenteras och, 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 om beslutet. *(FIB 2010:2)*

3 § Om det i ett avtal för visst internationellt samarbete förekommer bestämmelser om IT-säkerhet 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. *(FIB 2010:2)*

15 kap. Undantag

1 § Försvarsmakten får medge undantag från bestämmelserna i denna författning.

Överbefälhavaren eller den han eller hon bestämmer fattar beslut i ärenden om undantag.

[3] Senaste lydelse av förutvarande 13 kap. 2 § FIB 2007:1.

Ikraftträdande- och övergångsbestämmelser

1. Denna författning[4] träder i kraft den 15 mars 2006.

2. Genom författningen upphävs Försvarsmaktens interna bestämmelser (FIB 2003:3) om IT-säkerhet.

3. 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.

Ska ett IT-system, på grund av förändringar som kan påverka säkerheten i det, på nytt ackrediteras ska dock föreskrifterna i 7 kap. 3 §, 8 kap. 1 §, 10 kap. 1 § och 11 kap. 1 § i den nya författningen tillämpas. *(FIB 2010:2)*

4. 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. *(FIB 2010:2)*

Denna författning[5] träder i kraft den 1 mars 2010.

Sverker Göranson

Stefan Ryding-Berg

[4] FIB 2006:2
[5] FIB 2010:2