FÖRSVARSMAKTENS INTERNA BESTÄMMELSER

FIB 2006:2
Utkom från
trycket
2006-02-16

Försvarsmaktens interna bestämmelser om IT-säkerhet;

beslutade den 9 februari 2006.

Försvarsmakten föreskriver följande.

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 som övriga uppgifter, om inget annat anges i denna författning.

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 skall fullgöras av varje organisationsenhet.

Definitioner

6 § I dessa bestämmelser avses med

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

2. *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,

3. *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,

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

5. *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,

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

7. *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,

8. *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,

9. *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,

10. *produktägare*: den som är processägare för ÖB ledningsprocess, huvudprocessägare eller stödprocessägare i Högkvarteret, eller chef för en organisationsenhet, eller den som överbefälhavaren bestämmer, och som har ansvaret för den verksamhet som ett IT-system huvudsakligen skall stödja, och

11. *systemägare:* den chef för en organisationsenhet som ansvarar för den del av ett IT-system som skall användas i den egna verksamheten.

7 § I 13 kap. 13 § Försvarsmaktens föreskrifter (FFS 2005:7) om verksamheten vid Försvarsmakten (verksamhetsordning) finns föreskrifter om Chief Information Officer (CIO, Försvarsmaktens sambands- och informationssystemchef).

Bemyndigande att vara produktägare i Högkvarteret

8 § Chefen för produktion får bemyndiga chefen för förbandsproduktion eller chefen för materielproduktion att vara produktägare i hans ställe.

Planer

9 § Varje organisationsenhet skall i en plan ange vilka åtgärder som skall vidtas vid avbrott eller störningar i IT-systemets funktion.

10 § Chefen för en organisationsenhet skall i en skriftlig plan (IT-säkerhetsplan) fastställa riktlinjer för IT-säkerheten inom organisationsenheten.

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

11 § Vid varje organisationsenhet skall 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 skall chefen för organisationsenheten överväga om det på den platsen behövs en biträdande IT-säkerhetschef.

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

2 kap. Rapportering

1 § Händelser som kan påverka säkerheten i och kring Försvarsmaktens IT-system skall omedelbart rapporteras till närmaste chef, organisationsenhetens IT-säkerhetschef, operativa enheten i Högkvarteret samt till militära underrättelse- och säkerhetstjänsten i Högkvarteret.

3 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 skall 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 skall 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 skall göra hot-, risk- och sårbarhetsanalyser. Sådana analyser skall även göras i fråga om övriga IT-system.

2 § Varje garnisonschef eller den han bestämmer skall genomföra och dokumentera hot-, risk- och sårbarhetsanalyser i fråga om ett IT-system som skall användas gemensamt inom garnisonen och utifrån analyserna vidta lämpliga skyddsåtgärder.

3 § Analyser som avses i 1 och 2 §§ i detta kapitel skall dokumenteras i säkerhetsmålsättningar.

4 § Varje organisationsenhet skall se till att skyddet i och kring ett IT-system som inte är avsett för behandling av hemliga uppgifter är tillfredsställande. Organisationsenheten skall dokumentera det skydd som finns i fråga om IT-systemet. Dokumentationen skall hållas aktuell.

5 § Varje organisationsenhet skall 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. 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 skall dokumenteras.

5 kap. Utbildning

1 § Chefen för en organisationsenhet skall, innan en person tilldelas behörighet att använda ett IT-system, se till att han eller hon på ett säkert sätt kan hantera systemet. Användaren skall ha genomgått erforderlig utbildning i IT-säkerhet

med godkänt resultat. Organisationsenheten skall föra en förteckning över vilka som har genomgått en sådan utbildning i IT-säkerhet.

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.

6 kap. Behörighetskontroll m.m.

1 § Chefen för en organisationsenhet eller den han bestämmer skall besluta vem som är behörig att använda eller ta del av uppgifter i ett IT-system.

Ett sådant beslut skall dokumenteras.

2 § Om kod eller kort eller båda ger behörighet till eller i ett IT-system skall kod respektive kort knytas till den individ som är behörig att använda eller ta del av uppgifter i systemet. Kod och kort skall hanteras på ett sådant sätt att någon obehörig person inte kan komma åt dem.

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 skall vara försett med en av myndigheten godkänd säkerhetsfunktion för behörighetskontroll. Även övriga IT-system som är avsedda att användas av flera personer skall vara försedda med en sådan godkänd säkerhetsfunktion.

Med myndighet enligt första stycket avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

7 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 skall vara försett med en av myndigheten godkänd säkerhetsfunktion för säkerhetsloggning. Även övriga IT-system som är avsedda att användas av flera personer skall vara försedda med en sådan godkänd säkerhetsfunktion.

Med myndighet enligt första stycket avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

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 skall dokumenteras.

3 § Produktägaren skall se till att säkerhetsloggen kan analyseras och att loggen har erforderlig detaljeringsgrad.

4 § Systemägaren eller den han bestämmer skall se till att säkerhetsloggar analyseras.

5 § Chefen för organisationsenheten skall se till att användare av ett IT-system informeras om att säkerhetsloggning sker.

6 § Varje säkerhetslogg vid organisationsenheten skall förvaras i läsbar form. Den skall fortlöpande kopieras och vårdas.

8 kap. Skydd mot röjande signaler och obehörig avlyssning

1 § Med myndighet som enligt 7 kap. 13 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd skall godkänna säkerhetsfunktioner för skydd mot röjande signaler och obehörig avlyssning avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

9 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 skall vara försett med en av myndigheten godkänd säkerhetsfunktion som skyddar mot intrång. Även övriga IT-system som är avsedda att användas av flera personer skall 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 skall godkänna en säkerhetsfunktion som möjliggör intrångsdetektering avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

10 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 skall vara försett med en av myndigheten godkänd säkerhetsfunktion som skyddar mot skadlig kod. Även övriga IT-system skall vara försedda med en sådan godkänd säkerhetsfunktion.

Med myndighet enligt första stycket avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

11 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 skall 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 skall 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 skall ackrediteras, om inte CIO eller den han bestämmer beslutar annat.

2 § Beslut om ackreditering skall dokumenteras.

3 § Produktägaren skall besluta i fråga om ackreditering av ett IT-system (central ackreditering). Produktägaren skall inför ett sådant beslut se till att säkerheten i och kring IT-systemet granskas.

Produktägaren skall se till att säkerheten granskas i och kring även sådana IT-system som inte skall ackrediteras, om inte CIO eller den han bestämmer beslutar annat.

Produktägaren skall se till att det vid säkerhetsgranskningen särskilt beaktas hur systemet är avsett att samverka med andra IT-system. En säkerhetsgranskning skall dokumenteras.

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 skall 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 skall militära underrättelse- och säkerhetstjänsten i Högkvarteret yttra sig i fråga om säkerheten i systemet, om inte CIO eller den han bestämmer beslutar annat.

5 § Systemägaren skall besluta i fråga om ackreditering av ett IT-system som skall användas i den egna verksamheten (lokal ackreditering).

Innan ett IT-system får ackrediteras lokalt skall det ha ackrediterats centralt. Produktägaren skall 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 skall användas gemensamt inom en garnison, skall han ha inhämtat samråd från garnisonschefen.

6 § Ett IT-system som är avsett för behandling av hemliga uppgifter och som har ackrediterats skall 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 skall 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 skall 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. Kontroll

1 § I 6 kap. Försvarsmaktens interna bestämelser (FIB 2005:2) om säkerhetskydd och skydd av viss materiel finns föreskrifter om var militära underrättelse- och säkerhetstjänsten i Högkvarteret skall genomföra säkerhetsskyddskontroller.

2 § Chefen för militära underrättelse- och säkerhetstjänsten i Högkvarteret skall leda sådan kontrollverksamhet som rör säkerheten i och kring IT-system som inte är avsedda för behandling av hemliga uppgifter. Militära underrättelse- och sä-

kerhetstjänsten samt operativa enheten i Högkvarteret får genomföra kontroller av säkerheten i och kring sådana IT-system vid organisationsenheterna.

3 § Chefen för en organisationsenhet skall 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.

4 § Kontroller som avses i 2 och 3 §§ i detta kapitel skall dokumenteras.

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.

13 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 § Chef för kontingent får för utlandsstyrkan fatta beslut som avviker från 7 kap. Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd och från denna författning, om det är oundgängligen nödvändigt för verksamheten. Detsamma gäller chef för organisationsenhet i fråga om övrig verksamhet som avses i 1 § i detta kapitel.

Beslut som avses i första stycket skall dokumenteras och, om möjligt, föregås av samråd med militära underrättelse- och säkerhetstjänsten i Högkvarteret. Har

sådant samråd inte skett skall militära underrättelse- och säkerhetstjänsten i Högkvarteret snarast underrättas om beslutet.

3 § Om det i ett avtal för visst internationellt samarbete förekommer bestämmelser om IT-säkerhet som avviker från bestämmelserna i denna författning skall bestämmelserna i avtalet ha företräde.

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

14 kap. Undantag

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

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

Ikraftträdande- och övergångsbestämmelser

1. Denna författning 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 6 kap. 3 §, 7 kap. 1 §, 9 kap. 1 § och 10 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 6 kap. 3 §, 7 kap. 1 §, 9 kap. 1 § och 10 kap. 1 § i den nya författningen tillämpas.

4. Har ett underlag för ackreditering tagits fram före den 1 januari 2004 gäller inte föreskrifterna i 6 kap. 3 §, 7 kap. 1 §, 9 kap. 1 § och 10 kap. 1 § i den nya författningen i fråga om detta underlag.

Håkan Syrén

Stefan Ryding-Berg