FÖRSVARSMAKTEN

FÖRSVARSMAKTENS INTERNA BESTÄMMELSER

FIB 2017:8
Utkom från trycket
2017-12-18

Försvarsmaktens interna bestämmelser om it-säkerhet;

beslutade den 15 december 2017.

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, 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.

4 § Vad som föreskrivs i Försvarsmaktens föreskrifter (FFS 2015:2) om säkerhetsskydd 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 och dokumentation ska fullgöras av varje organisationsenhet.

Definitioner

6 § I dessa bestämmelser avses med

1. *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,
2. *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,
3. *central ackreditering:* beslut om ackreditering av ett it-system,
4. *elektroniskt kommunikationsnät:* 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,
5. *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,
6. *it-system:* system av sammansatt hård- och mjukvara som hanterar information,
7. *lokal ackreditering:* beslut av en chef för en organisationsenhet om ackreditering av ett it-system som ska användas i den egna verksamheten,
8. *sekretessklassificerad handling:* en handling som innehåller sekretessklassificerad uppgift,

9. *sekretessklassificerad uppgift (SK):* en uppgift som är sekretessbelagd enligt offentlighets- och sekretesslagen men som inte rör rikets säkerhet och som inte är en utrikesklassificerad uppgift,

10. *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,

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

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

13. *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,

14. *utrikesklassificerad uppgift (UK):* en uppgift som av en utländsk myndighet eller en mellanfolklig organisation eller av en svensk myndighet 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.

Planer

7 § Chefen för en organisationsenhet ska i en skriftlig plan (it-säkerhetsplan) fastställa vilka it-säkerhetsåtgärder som ska vidtas inom organisationsenheten.

It-säkerhetschef och biträdande it-säkerhetschef

8 § 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.

2 kap. It- säkerhetsrapportering

1 § Händelser som kan påverka säkerheten negativt i och kring Försvarsmaktens it-system ska omedelbart rapporteras till lokal säkerhetsorganisation eller närmaste chef.

Den som har tagit emot en sådan it-säkerhetsrapport ska se till att den vidarebefordras till:

- den regionala stab som den rapporterande organisationsenheten tillhör,
- it-säkerhetsansvarig för aktuellt it-system,
- it-försvarsförbandet vid Försvarsmaktens telekommunikations- och informationssystemförband,
- ledningsstaben i Högkvarteret,
- produktionsledningen i Högkvarteret,
- insatsledningen i Högkvarteret, och
- den militära underrättelse- och säkerhetstjänsten i Högkvarteret.

Chefen för den militära underrättelse- och säkerhetstjänsten i Högkvarteret får besluta att it-säkerhetsrapporter ska rapporteras på annat sätt.

3 kap. Hantering av lagringsmedium för hemliga uppgifter

1 § Ett lagringsmedium ska registreras om det kan tillföras uppgifter kontinuerligt och är avsett att innehålla eller innehåller uppgifter som är placerade i informationssäkerhetsklass HEMLIG/RESTRICTED.

I registret ska anges:

- lagringsmediets unika identifieringsuppgift,
- vem som har tilldelats lagringsmediet, och
- om lagringsmediet har återlämnats, förstörts eller förkommit.

2 § Ett lagringsmedium som kan tillföras uppgifter kontinuerligt ska kvitteras av användaren vid mottagandet om det är

1. avsett för personligt eller gemensamt tjänstebruk, och
2. placerat i informationssäkerhetsklass HEMLIG/RESTRICTED.

Kvittering ska ske genom namnteckning och namnförtydligande. Ett namnförtydligande får vara en kod.

Kravet på kvittering gäller inte för

1. personal som arbetar med drift av it-system när personalen hanterar lagringsmedium som har tilldelats eller ska tilldelas andra personer, och

2. arkiv-, expeditions- eller sambandspersonal som tar emot ett lagringsmedium för registrering, distribution, arkivering, förstöring eller in- och utläsning.

4 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 interna bestämmelser (FIB 2015:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

2 § Ett lagringsmedium som innehåller sekretessklassificerade uppgifter får återanvändas om åtgärder har vidtagits för att säkerställa att uppgifter inte längre kan utläsas ur lagringsmediet.

Chefen för militära underrättelse- och säkerhetstjänsten i Högkvarteret, eller den han eller hon bestämmer, beslutar om vilka åtgärder som krävs för att ett lagringsmedium ska få återanvändas.

3 § Förstöring av ett lagringsmedium som innehåller sekretessklassificerade uppgifter som får förstöras ska ske så att åtkomst och återskapande av uppgifterna försvåras.

Chefen för militära underrättelse- och säkerhetstjänsten i Högkvarteret, eller den han eller hon bestämmer, beslutar om krav på åtgärder för förstöring.

5 kap. Utveckling, anskaffning, användning och avveckling

1 § Det ska för varje it-system finnas en it-säkerhetsansvarig under hela systemets livscykel. Den it-säkerhetsansvarige ska se till att upprätta och vidmakthålla säkerheten i och kring systemet.

2 § Utöver vad som följer av föreskrifterna om analys i 7 kap. 7 § Försvarsmaktens föreskrifter (FFS 2015:2) om säkerhetsskydd, ska varje organisationsenhet som överväger att införa eller använda ett it-system noga analysera vilket skydd ett sådant system kräver och vilka åtgärder som måste vidtas för att skyddet ska få avsedd effekt. En sådan analys ska även omfatta en hot-, risk- och sårbarhetsanalys.

Detsamma gäller innan ett sådant it-system upplåts till en annan myndighet, ett annat land eller en mellanfolklig organisation.

Analyserna ska dokumenteras i säkerhetsmålsättningar.

3 § Inom ramen för garnisonssamordning ska en dokumenterad hot-, risk- och sårbarhetsanalys genomföras för ett it-system som ska användas gemensamt av flera organisationsenheter. Utifrån analysen ska lämpliga skyddsåtgärder vidtas.

4 § Chefen för en organisationsenhet ska se till att skyddet i och kring ett lokalt ackrediterat it-system som inte är avsett för behandling av hemliga uppgifter är tillfredsställande. Chefen för organisationsenheten ska se till att dokumentera det skydd som finns i fråga om it-systemet. Dokumentationen ska hållas aktuell.

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.

6 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 den som fattat beslut om central ackreditering 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.

7 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.

Vid organisationsenheten ska det föras 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.

8 kap. Behörighetstilldelning

1 § Behörighet till it-system och it-tjänster ska tilldelas den som behöver tillgång till systemet eller till tjänsten, för sin tjänst.

Behörighet i it-system och it-tjänster ska endast avse den information och de funktioner som användaren behöver för att utföra sitt arbete.

2 § Chefen för en organisationsenhet eller den han eller hon bestämmer ska besluta vem som är behörig att använda eller ta del av uppgifter i ett it-system.

Ett sådant beslut ska dokumenteras.

3 § 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.

4 § I 7 kap. 10 § Försvarsmaktens föreskrifter (FFS 2015:2) 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 avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

9 kap. Säkerhetsloggning

1 § I 7 kap. 11 § Försvarsmaktens föreskrifter (FFS 2015:2) 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 avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

2 § En säkerhetslogg får stängas av endast om det är oundgängligen nödvändigt.

Anledning till avstängningen, vem som har fattat beslutet, tidpunkten för avstängningen och, om så har skett, tidpunkten för återstarten av loggen ska dokumenteras.

3 § En säkerhetslogg ska ha erforderlig detaljeringsgrad och analyseras.

4 § Chefen för en organisationsenhet ska se till att användare av ett it-system informeras om att säkerhetsloggning sker.

5 § Varje säkerhetslogg vid organisationsenheten ska förvaras i läsbar form. Den ska fortlöpande kopieras och vårdas.

10 kap. Skydd mot röjande signaler och obehörig avlyssning

1 § Med myndighet som enligt 7 kap. 13 § Försvarsmaktens föreskrifter (FFS 2015:2) om säkerhetsskydd ska godkänna säkerhetsfunktioner för skydd mot röjande signaler och obehörig avlyssning, avses militära underrättelse- och säkerhetstjänsten i Högkvarteret.

11 kap. Intrångsskydd och intrångsdetektering

1 § Med myndighet enligt 7 kap. 14 § Försvarsmaktens föreskrifter (FFS 2015:2) om säkerhetsskydd avses militära underrättelse- och säker-hetstjänsten i Högkvarteret.

2 § Av 7 kap. 14 § Försvarsmaktens föreskrifter (FFS 2015:2) 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.

En sådan säkerhets-funktion beslutas av den militära underrättelse- och säkerhetstjänsten i Högkvarteret.

12 kap. Skydd mot skadlig kod

1 § I 7 kap. 15 § Försvarsmaktens föreskrifter (FFS 2015:2) 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 avses militära underrättelse- och säker-hetstjänsten i Högkvarteret.

13 kap. Ackreditering

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 FM CIO eller den han eller hon bestämmer beslutar annat.

2 § Beslut om ackreditering ska dokumenteras.

3 § FM CIO, eller den han eller hon bestämmer, beslutar om central ackreditering.

Inför ett beslut om central ackreditering ska säkerheten i och kring it-systemet granskas.

Säkerheten ska granskas i och kring även sådana it-system som inte ska ackrediteras, om inte FM CIO, eller den han eller hon bestämmer, beslutar annat.

Vid säkerhetsgranskningen ska det särskilt beaktas hur systemet är avsett att samverka med andra it-system.

En säkerhetsgranskning ska dokumenteras.

4 § Innan ett it-system som 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.

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 FM CIO, eller den han eller hon bestämmer, beslutar om annat.

5 § Chefen för en organisationsenhet ska besluta om lokal ackreditering.

Innan ett it-system får ackrediteras lokalt ska det ha ackrediterats centralt. Den som beslutat om central ackreditering ska se till att chefen för organisationsenheten förses med erforderligt underlag och erforderliga resurser för den lokala ackrediteringen.

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 FM CIO eller den han eller hon bestämmer beslutar annat.

It-system som enligt beslut av FM CIO, eller den han eller hon har bestämt, inte har ackrediterats ska ackrediteras om det sker förändringar i eller kring systemet som kan påverka dess säkerhet, om inte FM CIO eller den han eller hon bestämmer beslutar annat.

14 kap. Kontroll

1 § I 6 kap. Försvarsmaktens interna bestämmelser (FIB 2015:2) om säkerhetsskydd och skydd av viss materiel finns föreskrifter om var militära underrättelse- och säkerhetstjänsten i Högkvarteret ska genomföra säkerhetsskyddskontroller.

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.

3 § Militära underrättelse- och säkerhetstjänsten samt insatsledningen i Högkvarteret får genomföra kontroller vid organisationsenheterna avseende säkerheten i och kring it-system som inte är avsedda för behandling av hemliga uppgifter.

4 § 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.

Chefen för en organisationsenhet får inom ramen för garnisonssamordning genomföra kontroller av säkerheten i och kring it-system som inte är avsedda för behandling av hemliga uppgifter.

5 § Kontroller som avses i 2–4 §§ ska dokumenteras.

6 § 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.

15 kap. Internationell verksamhet

1 § Bestämmelserna i detta kapitel gäller när Försvarsmakten

1. deltar i en internationell militär insats och förberedelse för sådan verksamhet,
2. deltar i internationell fredsfrämjande verksamhet eller annat internationellt samarbete samt i utbildning eller förberedelser för sådan verksamhet eller samarbete, och
3. deltar i förevisningar av materiel eller verksamhet utomlands.

2 § Chef för en kontingent i en internationell militär insats får, i fråga om verksamhet utanför Sverige, fatta beslut som avviker från 7 kap. Försvarsmaktens föreskrifter (FFS 2015:2) 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 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.

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 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.

16 kap. Undantag

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

Överbefälhavaren, eller den han eller hon bestämmer, beslutar i ärenden om undantag.

---

1. Denna författning träder i kraft den 1 februari 2018.

2. Genom författningen upphävs Försvarsmaktens interna bestämmelser (FIB 2006:2) om IT-säkerhet.

3. Har ett beslut enligt 15 kap. 2 § fattats före ikraftträdande av denna författning, ska beslutet gälla som ett beslut i enlighet med denna författning.

Micael Bydén

Carin Bratt