Polismyndighetens författningssamling

ISSN 2002-0139
Utgivare: Gunilla Svahn Lindström

Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd;

PMFS 2015:3

Utkom från trycket
den 23 april 2015

beslutade den 24 mars 2015.

Säkerhetspolisen föreskriver följande med stöd av 43 och 44 §§ säkerhetsskyddsförordningen (1996:633) och meddelar följande allmänna råd.

1 kap. Allmänna bestämmelser

1 § Dessa föreskrifter gäller för de statliga myndigheter som avses i 39 § 2 säkerhetsskyddsförordningen (1996:633) och för kommuner och landsting. Bestämmelserna om registerkontroll i 8 kap. gäller även för Regeringskansliet och för myndigheter som avses i 39 § 1 samt bolag som avses i 19 § tredje stycket säkerhetsskyddsförordningen.

2 § Vad som i dessa föreskrifter föreskrivs om myndigheter gäller också för kommuner och landsting.

3 § I dessa föreskrifter avses med handling detsamma som anges i 2 kap. 3 § tryckfrihetsförordningen (1949:105). Med hemlig uppgift, hemlig handling och säkerhetskänslig verksamhet avses detsamma som anges i 4 § säkerhetsskyddsförordningen (1996:633).

4 § Vad som föreskrivs om hemlig handling gäller även för handling som är av synnerlig betydelse för rikets säkerhet, s.k. kvalificerat hemlig handling, om inte annat särskilt anges.

Med hemlig handling avses, om inte annat anges, såväl allmän som icke allmän handling.

5 § I en säkerhetsanalys enligt 5 § säkerhetsskyddsförordningen (1996:633) ska myndigheten även ange om myndigheten anser att det föreligger behov av att anta ytterligare föreskrifter enligt 45 § säkerhetsskyddsförordningen.

Av säkerhetsanalysen bör framgå vilka IT-system som behandlar uppgifter som är av betydelse för rikets säkerhet och vilka IT-system som är i behov av skydd mot terrorism.

6 § En myndighet ska se till att säkerhetsskyddet anpassas till verksamhetens art, omfattning och övriga omständigheter samt, i fråga om hemliga uppgifter, till vilken säkerhetsskyddsnivå uppgiften hör.

7 § Fel och brister i säkerhetsskyddet, vilka inte är av endast ringa betydelse, ska snarast åtgärdas och anmälas till myndighetens säkerhetsskyddschef eller, om sådan inte finns, till myndighetens chef eller motsvarande organ.

2 kap. Allmänt om informationssäkerhet

1 § Bestämmelser om vem som är behörig att ta del av hemliga uppgifter finns i 7 § säkerhetsskyddsförordningen (1996:633).

Myndighetens chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer ska besluta om vem som är behörig att ta del av kvalificerat hemliga uppgifter.

2 § I 13 § säkerhetsskyddsförordningen (1996:633) finns bestämmelser om vad som gäller när hemliga uppgifter skickas elektroniskt.

3 § För signalskyddstjänsten gäller särskilda bestämmelser i fråga om hantering av kryptonycklar och signalskyddsmateriel samt användning av kryptografiska funktioner.

4 § Bestämmelser om informationssäkerhet för hemliga handlingar i skrift eller bild samt för hemliga uppgifter i IT-system finns i 3 kap. respektive 4 kap.

5 § Med *materiel* avses konstruktioner, maskiner, utrustning, lagringsmedium och liknande.

Med *lagringsmedium* avses såväl digitalt lagringsmedium som andra lagringsmedia, dock inte sådana handlingar i skrift eller bild som regleras i 3 kap.

Med *digitalt lagringsmedium* avses lagringsmedium som är avsett för annat än tillfällig lagring av digital information, exempelvis hårddiskar, disketter och USB-minnen.

Med *annat lagringsmedium* avses exempelvis analogt videogram, analogt ljudband och mikrofilm.

6 § Särskilda bestämmelser om hantering av digitala lagringsmedier finns i 4 kap. 32–33 §§. I övrigt ska ett lagringsmedium som innehåller eller har innehållit hemliga uppgifter hanteras på samma sätt som hemliga handlingar i skrift eller bild. I den mån sådan hantering inte är möjlig, ska myndigheterna vidta andra åtgärder så att säkerhetsskyddet blir jämförbart med det som finns för hemliga handlingar i skrift eller bild.

Ett lagringsmedium ska ha ett säkerhetsskydd som motsvarar den högsta säkerhetsskyddsnivå som krävs för såväl de enskilda uppgifterna som den totala mängden hemliga uppgifter på lagringsmediet.

7 § Annat materiel som innehåller hemliga uppgifter ska hanteras på samma sätt som hemliga handlingar i skrift eller bild. I den mån sådan hantering inte är möjlig, ska myndigheterna vidta andra åtgärder så att säkerhets-

skyddet blir jämförbart med det som finns för hemliga handlingar i skrift eller bild.

3 kap. Informationssäkerhet för hemliga handlingar i skrift eller bild

Hemligbeteckning

1 § En allmän hemlig handling i skrift eller bild ska på första sidan förses med särskild anteckning (hemligbeteckning).

En icke allmän hemlig handling i skrift eller bild ska på första sidan förses med en anteckning om att den är hemlig. Sådan anteckning ska utformas på lämpligt sätt.

Allmänna råd

Begreppet hemligbeteckning ska inte sammanblandas med begreppet sekretessmarkering. Bestämmelser om sekretessmarkering finns i offentlighets- och sekretesslagen (2009:400).

2 § En hemligbeteckning på en handling i skrift eller bild ska ha en rektangulär ram. Ramen ska vara enkel för hemlig handling och dubbel för kvalificerat hemlig handling.

Allmänna råd

Den rektangulära ramen bör vara röd.

3 § Om en hemlig handling i skrift eller bild består av flera sidor, ska på varje sida finnas en hänvisning till hemligbeteckningen eller anteckningen på första sidan.

4 § Om en handling i skrift eller bild som är försedd med hemligbeteckning inte längre bedöms vara hemlig, ska detta antecknas på handlingen. Anteckningen ska innehålla uppgift om myndighetens namn, datum för anteckningen och vem som fattat beslut i saken. Hemligbeteckningen ska där efter överkorsas. Åtgärden ska antecknas i det register där handlingen är diarieförd.

Om en handling i skrift eller bild som har försetts med den hemligbeteckning som gäller för en kvalificerat hemlig handling inte längre bedöms vara kvalificerat hemlig, ska samråd ske med den som upprättat handlingen innan åtgärder vidtas enligt första stycket. Anteckning om samrådet ska ske på handlingen.

Om en handling i skrift eller bild som är försedd med anteckning enligt 1 § tredje stycket inte längre bedöms vara hemlig, ska anteckningen överkorsas. På handlingen ska vidare anges vem som beslutat om överkorsningen.

Allmänna råd

Vid osäkerhet om en hemlig handling i skrift eller bild, som inte är kvalificerat hemlig, inte längre ska bedömas vara hemlig är det lämpligt att kontakt tas med den myndighet som upprättat handlingen.

Arbetsrutiner för hemlig handling i skrift eller bild

5 § Av sändlista eller särskild förteckning ska framgå hur många exemplar av en allmän hemlig handling i skrift eller bild som har framställts och vilka som är mottagare av dessa.

6 § Vid framställning av en allmän hemlig handling i skrift eller bild ska på första sidan antecknas handlingens beteckning, exemplarnummer, antal sidor samt eventuella bilagor. Sidorna ska numreras i följd. Av bilaga och blad i bok med lösbladssystem ska framgå till vilken handling bilagan respektive bladet hör.

7 § När en kopia av eller ett utdrag ur en allmän hemlig handling i skrift eller bild görs, ska detta antecknas på handlingen eller i en särskild förteckning. Det ska också antecknas till vem kopian eller utdraget har lämnats.

På utdrag ur allmän hemlig handling i skrift eller bild ska antecknas från vilken handling och vilka sidor det gjorts, om inte detta framgår av utdraget. Numrering ska ske enligt vad som föreskrivs i 6 §.

Allmänna råd

En myndighet bör i särskilda föreskrifter ange vilka rutiner som ska tillämpas i samband med kopiering av eller utdrag ur en icke allmän hemlig handling i skrift eller bild.

8 § Kopia av eller utdrag ur en kvalificerat hemlig handling i skrift eller bild får göras endast efter medgivande av myndighetens chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer.

Kvittering

9 § Den som tar emot en allmän hemlig handling i skrift eller bild ska kvittera mottagandet med namnteckning och namnförtydligande i register eller liggare eller på särskilt kvitto. Kvittensen ska bevaras hos myndigheten i minst 10 år.

Den som tar emot en icke allmän hemlig handling i skrift eller bild ska på begäran kvittera mottagandet enligt vad som föreskrivs i första stycket. Den som tar emot en kvalificerat hemlig handling i skrift eller bild ska kvittera mottagandet med namnteckning och namnförtydligande på särskilt kvitto. Kvittot ska upprättas i två exemplar. Om en sådan handling återlämnas, ska detta antecknas på kvittot. Kvittensen ska bevaras hos myndigheten i minst 25 år.

Vad som sägs i första och andra stycket gäller inte när arkiv- eller expeditionspersonal tar emot sådan hemlig handling för registrering, kopiering, arkivering eller förstöring, om inte den som lämnar över handlingen begär det.

Allmänna råd

En myndighet bör i särskilda föreskrifter ange hur kvitterade hemliga handlingar i skrift eller bild ska lämnas tillbaka.

10 § Om uppgifter i en kvalificerat hemlig handling i skrift eller bild lämnas muntligen eller genom visning, ska kvittering eller anteckning om att uppgifter lämnats ske.

En myndighet ska fastställa rutiner för hur en sådan kvittering eller anteckning ska ske.

Förvaring

11 § En hemlig handling i skrift eller bild ska förvaras i ett förvaringsutrymme med en sådan skyddsnivå att den inte obehörigen röjs, ändras eller förstörs. Skyddsnivån ska motsvara lägst säkerhetsskåp Svensk Standard SS 3492.

En myndighet får dock i särskilda föreskrifter bestämma att hemliga handlingar i skrift eller bild, som inte är kvalificerat hemliga, under en kortare tid av en arbetsdag får förvaras i låst arbetsrum under förutsättning att huvudnycklar och reservnycklar förvaras så att någon obehörig inte kan komma åt dem.

Ytterligare säkerhetsskyddsåtgärder för förvaringen ska vidtas, om myndighetens säkerhetsanalys ger anledning till det.

Allmänna råd

För att skydda hemliga handlingar i skrift eller bild från exempelvis förstöring genom brand kan myndigheten använda säkerhetsskåp Svensk Standard SS 3493.

12 § För förvaring av allmänna handlingar i arkivlokaler gäller för statliga myndigheter, utöver vad som föreskrivs i 11 §, de föreskrifter och allmänna råd som meddelas av Riksarkivet.

13 § En kvalificerat hemlig handling i skrift eller bild ska förvaras av myndighetens chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer.

14 § I ett register där en allmän hemlig handling i skrift eller bild är diarieförd ska framgå var handlingen förvaras eller om den kommit bort eller gallrats.

Medförande av hemliga handlingar utanför myndighetens lokaler

15 § När en hemlig handling i skrift eller bild medförs från myndighetens lokaler ska den hållas under omedelbar uppsikt eller förvaras på ett sätt som motsvarar den säkerhetsskyddsnivå som gäller för förvaringen av handlingen inom myndighetens lokaler.

En kvalificerat hemlig handling får inte medföras från myndighetens lokaler utan tillstånd av myndighetens chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer.

Inventering

16 § Inventering av allmänna hemliga handlingar i skrift eller bild ska protokollföras.

Allmänna råd

Med hänsyn till att preskriptionstiden för vårdslöshet med hemlig uppgift (19 kap. 9 § brottsbalken) är två år, bör hemliga handlingar i skrift eller bild, oavsett om de är kvalificerat hemliga eller inte, inventeras minst en gång per år.

Gallring

17 § För gallring av allmänna handlingar gäller för statliga myndigheter särskilda bestämmelser som meddelas av Riksarkivet.

Förstöring av hemliga handlingar i skrift eller bild

18 § Förstöring av en hemlig handling i skrift eller bild ska ske så att åtkomst och återskapande av uppgifterna omöjliggörs.

Förstöringen ska dokumenteras.

Arbetsrutiner vid distribution av hemliga handlingar

19 § En försändelse med hemliga handlingar i skrift eller bild ska sändas som värdepost, rekommenderad post eller motsvarande och med en av myndigheten godkänd distributör.

Allmänna råd

En myndighet bör i särskilda föreskrifter ange hur hemliga handlingar i skrift eller bild ska sändas och tas emot inom myndigheten.

20 § Den som hämtar en försändelse hos en distributör ska kontrollera att försändelsen överensstämmer med kvittenslistan och att försändelsen är oskadad. Vid skada ska den som hämtar försändelsen anmäla skadan hos avsändaren samt begära att distributören gör anteckning om skadans beskaffenhet.

21 § Mottagaren av försändelsen ska kontrollera att den 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. Görs ingen anmärkning, ska eventuella sigillavtryck förstöras.

22 § Bestämmelser om vad som ska ske om en hemlig uppgift kan ha röjts finns i 10 § säkerhetsskyddsförordningen (1996:633).

23 § I 11 § första stycket säkerhetsskyddsförordningen (1996:633) anges hur försändelser till utlandet ska sändas.

En hemlig handling i skrift eller bild som sänds utomlands ska förses med anteckning om uppgifternas ursprungsland.

En myndighet får besluta att personal vid myndigheten, som är behörig enligt 7 § säkerhetsskyddsförordningen (1996:633), får ta med försändelser med hemliga handlingar i skrift eller bild till utlandet.

Undantag

24 § En myndighet får i särskilda föreskrifter i fråga om hemliga handlingar i skrift eller bild, vars röjande endast kan antas medföra ringa men för rikets säkerhet, föreskriva om undantag från 3 kap. 5–7 och 9 §§, 11 § första stycket andra meningen, 14 §, 16 §, 18 § andra stycket och 20–21 §§. I dessa föreskrifter ska även anges hur sådana handlingar ska märkas.

Allmänna råd

Vid osäkerhet om konsekvenserna av ett röjande bör en hemlig handling i skrift eller bild hanteras enligt de ordinarie reglerna för sådan handling.

4 kap. Informationssäkerhet för IT-system

Definitioner

1 § I detta kapitel avses med

elektronisk handling: upptagning för automatiserad behandling,

IT-system: ett informationsbehandlingssystem som baseras på informationsteknik,

intrångsdetektering: administrativa eller tekniska åtgärder som vidtas för att detektera intrång eller försök eller förberedelse till intrång,

intrångsskydd: administrativa eller tekniska åtgärder som vidtas för att skydda IT-system mot obehörig åtkomst från ett elektroniskt kommunikationsnät,

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,

säkerhetsloggning: manuell eller automatisk registrering av händelser som är av betydelse för säkerheten i eller kring ett IT-system, och

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.

Allmänt om säkerhetsskyddet i IT-system

2 § Hemliga uppgifter och kvalificerat hemliga uppgifter får hanteras endast i IT-system som godkänts för sådan hantering av den myndighet för vars verksamhet systemet inrättats.

3 § En myndighet ska fastställa mål och riktlinjer för IT-säkerheten när det gäller IT-system som är avsedda för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism. Sådana mål och riktlinjer ska fastställas av myndighetens chef eller motsvarande organ och dokumenteras.

4 § En myndighet ska fastställa instruktioner för användning, förvaltning och drift av IT-system som är avsedda för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism. Sådana instruktioner ska fastställas av myndighetens chef eller motsvarande organ och dokumenteras.

Anskaffning, användning, utveckling, m.m.

5 § En myndighet som överväger att anskaffa, använda, utveckla eller förändra ett IT-system ska göra en översiktlig analys av vilket säkerhetsskydd systemet kräver.

6 § En myndighet ska av säkerhetsskäl avstå från ett IT-system eller begränsa dess innehåll, om erforderligt säkerhetsskydd inte kan uppnås.

7 § En myndighet som beslutar att anskaffa, använda, utveckla eller förändra ett IT-system, som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism, ska noga analysera de säkerhetsrisker och de sårbarheter som finns i och kring systemet. Analysen ska resultera i en sammanställning över de åtgärder som ska vidtas för att erforderligt säkerhetsskydd ska upprätthållas i och kring IT-systemet. En sådan analys ska dokumenteras.

I fråga om ett IT-system, som är avsett för behandling av hemliga uppgifter, ska vid analysen göras en bedömning av behovet av säkerhetsskydd avseende såväl de enskilda uppgifterna som den totala mängden hemliga uppgifter som kan komma att behandlas i systemet.

Vad som sägs i första stycket ska tillämpas även innan en myndighet upplåter ett IT-system till en annan myndighet, en annan stat eller en mellanfolklig organisation.

8 § En myndighet ska svara för att ett betryggande säkerhetsskydd upprätthålls i och kring ett IT-system, från dess anskaffning till dess avveckling.

9 § En myndighet ska dokumentera det säkerhetsskydd som finns i fråga om ett IT-system, från dess anskaffning till dess avveckling. Sådan dokumentation ska hållas aktuell.

10 § En myndighet som förvaltar ett IT-system, som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism och som är avsett att användas av en annan myndighet, en annan stat eller en mellanfolklig organisation, ska upprätta dokumentation avseende drift, förvaltning och säkerhet.

11 § Bestämmelser om krav på driftsgodkännande för IT-system, som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer, finns i 12 § tredje stycket säkerhetsskyddsförordningen (1996:633).

Inför ett sådant godkännande ska även säkerheten kring IT-systemet granskas. Därvid ska särskilt beaktas hur IT-systemet är avsett att samverka med andra system. En myndighet som inrättar ett sådant IT-system ska dokumentera resultatet av den granskning som skett och beslutet om godkännande av drift.

Allmänna råd

Bestämmelsen i 11 § bör tillämpas även i fråga om IT-system som särskilt behöver skyddas mot terrorism.

12 § En okrypterad dataförbindelse får användas för hemliga uppgifter inom ett område eller en lokal som disponeras av en myndighet först sedan myndigheten vidtagit betryggande åtgärder mot obehörig avlyssning.

Systemsäkerhetsansvarig

13 § För ett IT-system, som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism, ska finnas en av myndighetens chef eller motsvarande organ utsedd person som ansvarar för säkerheten i systemet.

Behörighetskontroll

14 § Ett IT-system, som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer, ska vara försett med tekniska eller administrativa åtgärder, eller både tekniska och administrativa åtgärder, för identifiering av användaren, verifiering av den föregivna identiteten, styrning av användarens åtkomsträttigheter till systemet samt registrering av användarens aktiviteter.

Allmänna råd

Bestämmelsen i 14 § bör tillämpas även i fråga om IT-system som särskilt behöver skyddas mot terrorism.

Ett IT-system, som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism och som är avsett att användas av flera personer, bör förses med ett förstärkt inloggningsskydd, exempelvis aktiva kort.

15 § Kod, lösenord eller motsvarande till IT-system, som är avsedda för behandling av hemliga uppgifter, ska ges ett säkerhetsskydd som motsvarar den högsta säkerhetsskyddsnivå som sådan information kan ge tillgång till.

Kod, lösenord eller motsvarande till IT-system, som särskilt behöver skyddas mot terrorism, ska förvaras så att någon obehörig inte kan komma åt dem.

Säkerhetsloggning

16 § I ett IT-system, som är avsett för behandling av hemliga uppgifter och som är avsett att användas av flera personer, ska loggning ske av användaridentitet, datum och tidpunkt för inloggning och utloggning samt sådana användaraktiviteter i övrigt som är av betydelse för säkerheten i systemet.

Allmänna råd

Bestämmelsen i 16 § bör tillämpas även i fråga om IT-system som särskilt behöver skyddas mot terrorism.

Exempel på användaraktiviteter som är av betydelse för säkerheten i ett IT-system är tillgång till berörda objekt (t.ex. filer eller registerposter) och övriga resurser (t.ex. skrivare) samt utförda operationer (t.ex. skapande, radering eller sökning).

17 § En myndighet ska besluta om hur ofta säkerhetsloggar ska analyseras, vad som ska analyseras och vem som ska ansvara för att sådan analys görs. En myndighet ska vidare besluta om hur länge säkerhetsloggar ska bevaras.

Beslut enligt denna bestämmelse ska dokumenteras.

18 § För gallring av allmänna handlingar gäller för statliga myndigheter särskilda bestämmelser som meddelas av Riksarkivet.

Skydd mot skadlig kod

19 § Ett IT-system, som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism, ska vara försett med av myndigheten godkänt skydd mot skadlig kod.

20 § En myndighet ska fastställa rutiner för uppdatering av skydd mot skadlig kod. Sådana rutiner ska dokumenteras.

Intrångsdetektering och skydd mot intrång

21 § Ett IT-system, som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism och som kommunicerar med

andra IT-system, ska vara försett med av myndigheten godkänt intrångsskydd och av myndigheten godkända funktioner för intrångsdetektering.

Ett IT-system som är avsett för behandling av hemliga uppgifter, vars röjande endast kan antas medföra ringa men för rikets säkerhet, behöver dock inte förses med funktioner för intrångsdetektering.

Skydd mot röjande signaler och obehörig avlyssning

22 § En myndighet ska analysera behovet av skydd mot röjande signaler från ett IT-system som är avsett för behandling av hemliga uppgifter. En sådan analys ska dokumenteras. Om det föreligger behov av sådant skydd, ska IT-systemet förses med skydd mot röjande signaler.

Ett IT-system, som är avsett för behandling av hemliga uppgifter, ska vara försett med ett betryggande skydd mot obehörig avlyssning.

Incidenthantering

23 § En myndighet ska fastställa rutiner för hantering, rapportering och uppföljning av incidenter av betydelse för säkerheten i eller kring ett IT-system, som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism. Sådana rutiner ska dokumenteras.

Säkerhetskopiering

24 § I ett IT-system, som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism, ska säkerhetskopiering ske.

En myndighet ska regelbundet kontrollera att informationen på säkerhetskopiorna går att återskapa.

25 § En säkerhetskopia ska förvaras avskilt från den plats där det IT-system från vilken kopian gjorts finns.

Kontinuitetsplan

26 § En myndighet ska besluta den längsta tid som ett IT-system, som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism, bedöms kunna vara ur funktion utan att verksamheten i väsentlig omfattning störs.

En myndighet ska i fråga om IT-system, som är avsett för behandling av hemliga uppgifter eller som särskilt behöver skyddas mot terrorism, besluta vilka reservrutiner som ska vidtas vid avbrott och störningar i IT-systemets funktion.

Beslut enligt denna bestämmelse ska dokumenteras.

Hantering av elektroniska hemliga handlingar

27 § En allmän hemlig elektronisk handling ska förses med särskild anteckning (hemligbeteckning). En icke allmän hemlig elektronisk handling

ska, om det kan ske utan större olägenhet, förses med anteckning om att den är hemlig. Sådan anteckning ska utformas på lämpligt sätt.

Allmänna råd

Begreppet hemligbeteckning ska inte sammanblandas med begreppet sekretessmarkering. Bestämmelser om sekretessmarkering finns i offentlighets- och sekretesslagen (2009:400).

En myndighet bör i särskilda föreskrifter ange i vilken utsträckning sådana handlingar som avses i 27 § andra stycket ska märkas.

En myndighet bör, för att uppfylla de i 3 kap. 5–6 §§ angivna kraven på ett enkelt sätt, använda mallkoncept eller dylikt så att de uppgifter som där krävs framgår av utskrivna dokument.

28 § Om en hemlig elektronisk handling, som försetts med hemligbeteckning eller anteckning enligt 27 § andra stycket, består av flera sidor ska, om det kan ske utan olägenhet, av varje sida framgå att den är hemlig.

29 § Om en hemlig elektronisk handling som är försedd med hemligbeteckning inte längre bedöms vara hemlig, ska hemligbeteckningen tas bort. På handlingen eller i särskild förteckning ska antecknas vilken myndighet som tagit bort markeringen, datum för åtgärden och vem som beslutat i saken. Åtgärden antecknas i det register där handlingen är diarieförd.

Om en kvalificerat hemlig elektronisk handling inte längre bedöms vara kvalificerat hemlig, ska samråd ske med den som upprättat handlingen innan åtgärder vidtas enligt första stycket. På handlingen eller i särskild förteckning ska antecknas att samråd skett.

Om en hemlig elektronisk handling som är försedd med anteckning enligt 27 § andra stycket inte längre bedöms hemlig, ska anteckningen tas bort. På handlingen eller i särskild förteckning ska antecknas vem som beslutat om åtgärden.

30 § En kvalificerat hemlig elektronisk handling får skickas elektroniskt inom myndigheten endast efter medgivande av myndighetens chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer.

31 § Inventering av allmänna hemliga elektroniska handlingar ska protokollföras.

Allmänna råd

En myndighet bör i särskilda föreskrifter ange

- i vilken omfattning kopiering av och utdrag ur en hemlig elektronisk handling får ske,
- om en hemlig elektronisk handling får skickas elektroniskt inom myndigheten och, om så är fallet, i vilken omfattning detta får ske,
- de rutiner som ska finnas för att kunna konstatera vem som fått del av en allmän hemlig elektronisk handling eller en kvalificerat hemlig elektronisk handling, och

– hur kvittering eller anteckning ska göras när uppgifter i en kvalificerat hemlig elektronisk handling lämnas muntligen eller genom visning.

Hantering av digitala lagringsmedium

32 § Ett digitalt lagringsmedium, som innehåller eller har innehållit hemliga uppgifter, får hanteras endast i ett IT-system som uppfyller de krav som gäller för den högsta säkerhetsskyddsnivå som krävs för någon av uppgifterna som finns eller har funnits på lagringsmediet.

33 § När ett digitalt lagringsmedium, som innehåller eller har innehållit hemliga uppgifter, medförs från myndighetens lokaler ska det hållas under omedelbar uppsikt eller förvaras på ett sätt som motsvarar den säkerhetsskyddsnivå som gäller för förvaringen av lagringsmediet inom myndighetens lokaler.

Första stycket behöver inte tillämpas, om uppgifterna på lagringsmediet krypterats med signalskyddssystem (kryptosystem) som har godkänts av Försvarsmakten (Högkvarteret).

5 kap. Tillträdesbegränsning

Allmänt

1 § En myndighet ska utfärda skriftligt besökstillstånd för utomstående personer som ska få tillträde till en plats där säkerhetskänslig verksamhet bedrivs eller som särskilt behöver skyddas mot terrorism. När personen besöker platsen ska hans eller hennes rätt att få tillträde kontrolleras.

2 § Vid alla passerställen till en plats, där säkerhetskänslig verksamhet bedrivs eller som särskilt behöver skyddas mot terrorism, ska finnas personell bevakning eller teknisk utrustning för tillträdeskontroll eller båda i kombination.

Allmänna råd

En myndighet bör i särskilda föreskrifter ange hur myndigheten reglerar tillträdesbegränsningen till platser där säkerhetskänslig verksamhet bedrivs eller som särskilt behöver skyddas mot terrorism.

Kort, koder och nycklar

3 § Kort, koder och nycklar till utrymmen där hemliga uppgifter finns, där säkerhetskänslig verksamhet bedrivs eller som särskilt behöver skyddas mot terrorism ska förvaras så att inte någon obehörig kan komma åt dem.

4 § Den som tilldelats ett förvaringsutrymme ska själv bestämma och, om möjligt, ställa in koden till förvaringsutrymmet.

5 § En myndighet ska ha en förteckning över samtliga kort, koder och nycklar som hör till förvaringsutrymmen där det finns hemliga uppgifter, där säkerhetskänslig verksamhet bedrivs eller som särskilt behöver skyddas mot terrorism. Av förteckningen ska det framgå till vem och när ett kort, en kod eller en nyckel har lämnats samt var reservkort, reservkod eller reservnyckel förvaras. Vidare ska framgå när ett kort, en kod eller en nyckel återlämnats.

6 § Om det kan befaras att ett kort eller en nyckel har förlorats eller kopierats, att en kod har röjts eller att ett kort, en kod eller en nyckel har använts av någon obehörig person, ska detta omedelbart anmälas till myndighetens säkerhetsskyddschef eller, om sådan inte finns, myndighetens chef eller motsvarande organ.

Allmänna råd

En myndighet bör i särskilda föreskrifter ange hur myndigheten reglerar tillträde till och ansvar för förvaringsutrymmen där hemliga uppgifter finns.

6 kap. Säkerhetsprövning

1 § Bestämmelser om säkerhetsprövning finns i 11 § säkerhetsskyddslagen (1996:627) och 14 § säkerhetsskyddsförordningen (1996:633).

2 § En myndighet ska undersöka vilka anställningar eller annat deltagande i verksamheten vid myndigheten som bör bli föremål för säkerhetsprövning. Resultatet av denna undersökning ska dokumenteras. Av dokumentationen ska framgå vilka anställningar m.m. som placerats i säkerhetsklass, vilka som innefattar en säkerhetsprövning utan att vara placerade i säkerhetsklass samt vilka anställningar eller annat deltagande i verksamheten som ska bli föremål för registerkontroll till skydd mot terrorism.

Allmänna råd

En myndighet bör fortlöpande pröva pålitligheten från säkerhetsskyddssynpunkt, särskilt i fråga om de personer som har anställning eller deltar i verksamhet som är placerad i säkerhetsklass eller som är registerkontrollerade till skydd mot terrorism.

7 kap. Säkerhetsskyddad upphandling med säkerhetsskyddsavtal

Allmänt

1 § Med företag avses i detta kapitel aktiebolag, handelsbolag, föreningar och andra juridiska personer samt enskilda firmor med vilka en myndighet avser att träffa avtal som avses i 8 § säkerhetsskyddslagen (1996:627).

2 § En myndighet ska innan en upphandling påbörjas pröva om denna helt eller delvis ska omges av säkerhetsskydd.

3 § Säkerhetsskyddet ska fortlöpande prövas och anpassas med hänsyn till aktuell hotbild, upphandlingens omfattning och skyddsvärdet hos de uppgifter som kommer att hanteras av det företag som upphandlas.

Bedömning av företagets lämplighet

4 § Innan en myndighet lämnar hemliga uppgifter till ett företag ska myndigheten göra en säkerhetsprövning och, i förekommande fall, låta göra en registerkontroll av företagets ledning och övriga inom företaget som avses få del av uppgifterna.

5 § Om ett företag ska hantera eller förvara hemliga uppgifter i egna lokaler, ska myndigheten genom besök kontrollera om företagets lokaler och övriga förhållanden är lämpliga från säkerhetsskyddssynpunkt.

Säkerhetsskyddsavtal och säkerhetsskyddsinstruktion

6 § Bestämmelser om när säkerhetsskyddsavtal ska ingås finns i 8 § säkerhetsskyddslagen (1996:627). Ett säkerhetsskyddsavtal som träffats inför en anbudsinfordran ska revideras i erforderlig utsträckning när avtal träffas om upphandling. När ett säkerhetsskyddsavtal har ingåtts ska företaget upprätta en säkerhetsskyddsinstruktion. Om företaget ska utföra arbete endast i myndighetens lokaler eller i lokaler som anvisats av myndigheten, får myndigheten medge att en sådan instruktion inte behöver upprättas. En säkerhetsskyddsinstruktion ska godkännas av myndigheten.

Slutförande av säkerhetsskyddsarbete

7 § När ett företag har fullgjort ett uppdrag som omgetts av säkerhetsskydd ska myndigheten säga upp säkerhetsskyddsavtalet.

Myndigheten ska säkerställa att vad som avtalats om tystnadsplikt och sekretess i övrigt ska bestå.

Underrättelse till Säkerhetspolisen

8 § En myndighet ska utan dröjsmål underrätta Säkerhetspolisen om säkerhetsskyddsavtal som träffats och om säkerhetsskyddsavtal som upphört att gälla.

En sådan underrättelse ska innehålla de uppgifter som framgår av blankett *Underlag säkerhetsskyddad upphandling* (SÄPO 070).

8 kap. Registerkontroll

Framställan om registerkontroll

1 § Framställan om registerkontroll görs hos Säkerhetspolisen.

Blanketter

2 § Framställan om registerkontroll ska innehålla de uppgifter som framgår av blanketten *Framställan om registerkontroll enligt säkerhetsskyddslagen* (SÄPO 072).

I fall där särskild personutredning ska göras enligt 18 § säkerhetsskyddslagen (1996:627) ska även de uppgifter som framgår av nedan angivna blankett anges.

1. Säkerhetsklass 1: blanketten *Särskild personutredning för säkerhetsklass 1 och 2* (SÄPO 073) och *Särskild personutredning för säkerhetsklass 1* (SÄPO 074).
2. Säkerhetsklass 2: blanketten *Särskild personutredning för säkerhetsklass 1 och 2* (SÄPO 073).

Framställan om registerkontroll beträffande dem som avses få del av hemliga uppgifter vid upphandling enligt 8 § säkerhetsskyddslagen (s.k. säkerhetsskyddad upphandling) ska ges in efter underrättelse om att avtal träffats enligt 7 kap. 8 §. Sådan framställan ska åtföljas av ett registreringsbevis för företaget. Registreringsbeviset får inte vara äldre än tre månader.

Samtycke

3 § Den som beslutar om registerkontroll ska dokumentera att samtycke till registerkontroll och, i förekommande fall, särskild personutredning inhämtats.

Kontrollorsak

4 § Vid registerkontroll ska kontrollorsaken anges så att det tydligt framgår vilken typ av verksamhet den kontrollerade avses delta i. Om uppdraget är tidsbegränsat, ska tiden anges.

Allmänna råd

Exempel på angivande av kontrollorsak är
- anställning som handläggare av beredskaps- och krigsplanläggningsfrågor,
- anställning som registrator med tillgång till en myndighets hemliga diarium,
- arbete som elektriker inom elförsörjningsområdet inom ramen för en säkerhetsskyddad upphandling, och
- besökstillstånd till anläggning där besökaren kommer att få del av hemliga uppgifter.

I offentlighets- och sekretesslagen (2009:400) finns bestämmelser om sekretess som är tillämpliga på uppgifter som lämnas ut vid registerkontroll och särskild personutredning. Det finns anledning att vara särskilt uppmärksam på frågor om sekretess när, enligt 25 § säkerhetsskyddslagen (1996:627), uppgifter lämnas ut utan att den kontrollerade har getts tillfälle att yttra sig över uppgifterna.

Återrapportering

5 § Den som beslutar om registerkontroll ska skyndsamt lämna Säkerhetspolisen besked om huruvida en person som genomgått sådan kontroll godkänts vid säkerhetsprövningen eller inte.

Ny kontroll

6 § Den som beslutar om registerkontroll ansvarar för att ny registerkontroll görs enligt 24–25 §§ säkerhetsskyddsförordningen (1996:633). Ny registerkontroll ska göras när den som har en befattning i säkerhetsklass 1 eller 2 har ingått äktenskap eller partnerskap eller inlett ett samboförhållande efter den senaste registerkontrollen.

Anmälan vid ändring av den kontrollerades förhållanden

7 § Den som beslutar om registerkontroll ska skriftligen underrätta Säkerhetspolisen, om en person har slutat i verksamhet som placerats i säkerhetsklass eller har övergått till verksamhet som placerats i lägre säkerhetsklass. Detsamma gäller, såvitt avser registerkontrollerade i säkerhetsklass 1 och 2, om den kontrollerades äktenskap eller partnerskap har upplösts eller om samboförhållandet har upphört.

8 § När en person har tagits i anspråk för uppgifter som normalt föranleder registerkontroll, men sådan kontroll har underlåtits med stöd av 16 § säkerhetsskyddslagen (1996:627), ska den som beslutat att underlåta kontroll skriftligen underrätta Säkerhetspolisen om detta. Skälen för sådan underlåtelse ska dokumenteras.

Kontaktperson

9 § Hos den som beslutar om registerkontroll ska finnas en kontaktperson som svarar för kontakterna med Säkerhetspolisen. Kontaktpersonen ska ha en ersättare.

9 kap. Utbildning och kontroll

Utbildning

1 § Bestämmelser om utbildning av personal i frågor om säkerhetsskydd finns i 30 § säkerhetsskyddslagen (1996:627).

Allmänna råd

Grundläggande utbildning bör ges till samtliga medarbetare på en arbetsplats som omfattas av säkerhetsskydd. Ytterligare utbildning bör ges till dem som direkt befattar sig med hemliga uppgifter eller som har sin arbetsplats förlagd på ett område där säkerhetskänslig verksamhet bedrivs eller som särskilt behöver skyddas mot terrorism.

2 § Vid en myndighet ska det finnas en plan för utbildning i säkerhetsskydd.

3 § En myndighet ska föra en förteckning över de anställda som har säkerhetsprövats och som har genomgått utbildning i säkerhetsskydd.

Kontroll

4 § Bestämmelser om kontroll av säkerhetsskyddet och tillsyn finns i 30 och 31 §§ säkerhetsskyddslagen (1996:627) samt i 39–42 §§ säkerhetsskyddsförordningen (1996:633).

5 § Vid en myndighet ska det finnas en plan för intern kontrollverksamhet.

6 § Kontroller ska ske fortlöpande och protokoll ska föras över genomförda kontroller. Protokollen ska förvaras samlade vid myndigheten.

10 kap. Internationella förhållanden

Allmänt

Allmänna råd

En myndighet bör vid utformandet av säkerhetsskyddet beakta inte enbart förevarande föreskrifter utan även sådana åtaganden som Sverige eller myndigheten gjort internationellt i fråga om säkerhetsskydd.

Hantering av internationella uppgifter

Allmänna råd

Om Sverige eller en myndighet i Sverige internationellt åtagit sig att säkerhetsskydda uppgifter som av annan stat, utländsk myndighet eller mellanfolklig organisation klassificerats som TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED eller motsvarande, bör dessa uppgifter, även om det inte är helt klarlagt att de utgör hemliga uppgifter i säkerhetsskyddslagstiftningens mening, hanteras som sådana uppgifter.

Utländska beteckningar

Allmänna råd

Om uppgifter hanteras som hemliga uppgifter, kan i allmänhet handlingar märkta TOP SECRET eller motsvarande hanteras som kvalificerat hemliga handlingar, SECRET eller motsvarande och CONFIDENTIAL eller motsvarande hanteras som hemliga handlingar och RESTRICTED eller motsvarande hanteras som hemliga handlingar vars röjande endast kan antas medföra ringa men för rikets säkerhet. Motsvarande gäller även för lagringsmedium och annat materiel som åsatts sådan utländsk beteckning.

Allmänna råd

Handlingar som upprättas i Sverige men är avsedda att sändas till annan stat, utländsk myndighet eller mellanfolklig organisation bör utöver eventuell svensk märkning åsättas relevant utländsk beteckning, såsom TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED eller motsvarande. Utländsk beteckning bör även åsättas andra handlingar som upprättas i Sverige, om Sverige eller en myndighet i Sverige internationellt åtagit sig att så ska ske. Motsvarande bör gälla för lagringsmedium och annat materiel. Vid åsättande av sådan utländsk beteckning bör respektive definition i tillämplig internationell överenskommelse beaktas. Utländsk beteckning bör utformas i enlighet med vad som föreskrivs i tillämplig internationell överenskommelse och, för det fall sådana föreskrifter saknas, på annat lämpligt sätt.

11 kap. Undantag

1 § Säkerhetspolisen får medge undantag från bestämmelserna i dessa föreskrifter.

Dessa föreskrifter och allmänna råd träder i kraft den 1 maj 2015, då Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd (RPSFS 2010:3, FAP 244-1) ska upphöra att gälla.

På Säkerhetspolisens vägnar

ANDERS THORNBERG

Kjell Cromnier
(Enheten för operativa åtgärder)