

Pliktverkets interna bestämmelser



Pliktverkets interna bestämmelser om säkerhetsskydd

PIB 2008:9

beslutade den 14 oktober 2008.

Pliktverket föreskriver följande med stöd av 45 § säkerhetsskyddsförordningen (1996:633).

1 kap. Tillämpningsområde och definitioner

1 § I dessa bestämmelser regleras Pliktverkets säkerhetsskydd.

2 § Inom Pliktverket omfattas säkerhetsskyddet av

- informationssäkerhet inklusive IT-säkerhet
- tillträdesbegränsning
- säkerhetsprovning
- utbildning
- kontroll
- säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA)
- signalskydd.

3 § I dessa bestämmelser gäller följande definitioner

- *hemlig uppgift*: en uppgift som omfattas av sekretess enligt sekretesslagen (1980: 100) och som rör rikets säkerhet
- *hemlig handling*: en handling som innehåller en hemlig uppgift
- *kvalificerat hemlig handling*: en hemlig handling som innehåller en uppgift som är av synnerlig betydelse för rikets säkerhet.

2 kap. Grundläggande bestämmelser

1 § De grundläggande bestämmelserna om säkerhetsskydd finns i säkerhetsskyddslagen (1996: 627), säkerhetsskyddsförordningen (1996: 633) och i Försvarmaktens föreskrifter (FFS 2003: 7) om säkerhetsskydd.

3 kap. Informationssäkerhet

1 § Informationssäkerhet avser det skydd som hindrar att uppgifter som omfattas av sekretess och som rör rikets säkerhet röjs, ändras eller förstörs.

2 § Säkerhetsskyddet är indelat i fyra informationssäkerhetsklasser.

1. Hemlig/Top Secret

Kvalificerat hemliga uppgifter som kan medföra synnerliga men för totalförsvaret om de röjs.

2. Hemlig/Secret
Hemliga uppgifter som kan medföra betydande men för totalförsvaret om de röjs.
3. Hemlig/Confidential
Hemliga uppgifter som kan medföra inte obetydliga men för totalförsvaret om de röjs.
4. Hemlig/Restricted
Hemliga uppgifter som kan medföra endast ringa men för totalförsvaret om de röjs.

3 § En hemlig handling ska placeras i en av de informationssäkerhetsklasser som är angivna i 2 §. Informationssäkerhetsklassen ska anges på handlingen. Om en hemlig handling består av flera sidor ska det på varje sida finnas en hänvisning till uppgiften om informationssäkerhetsklass på första sidan.

Kompletterande bestämmelser

4 § Pliktverkets interna bestämmelser om IT-säkerhet innehåller kompletterande bestämmelser om informationsskydd vid automatisk informationsbehandling. I Pliktverkets expeditionshandbok finns anvisningar för framställning, hemligstämpling och märkning av databärare som innehåller eller har innehållit en hemlig uppgift.

Materiel som jämföras med hemliga handlingar

5 § Informationstekniksystem, disketter, cd-skivor, hårddiskar, minneskort och dylikt ska jämföras med hemliga handlingar och hanteras på samma sätt om de innehåller eller har innehållit en hemlig uppgift.

Behörighet att hantera eller ta del av hemliga uppgifter

6 § Avdelningschefen, eller den han eller hon utser, beslutar skriftligt om vem som är behörig att hantera en hemlig eller kvalificerat hemlig handling eller ta del av en hemlig uppgift som är placerad i någon av informationssäkerhetsklasserna Hemlig/Confidential, Hemlig/Secret eller Hemlig/Top Secret. Vid avdelningen för personalredovisning och verksamhetsstöd ska det finnas en lista med namnen på de personer som har rätt att hantera eller ta del av hemliga handlingar och hemliga uppgifter.

7 § Den som får ta del av en hemlig uppgift ska först informeras om vad sekretessen innebär och omfattar. Säkerhetsskyddschefen fastställer omfattningen av den information som ska lämnas till arbetstagaren. Avdelningschefen ska se till att arbetstagaren får informationen och att ett sekretessbevis utfärdas.

8 § Hemliga uppgifter får inte avhandlas muntligt eller visas annat än i en lokal eller inom ett område där säkerheten är godkänd.

Kvittering av hemliga handlingar

9 § Hemliga handlingar i informationssäkerhetsklasserna Hemlig/Confidential, Hemlig/Secret eller Hemlig/Top Secret ska alltid kvitteras med namnteckning och namnförtydligande.

10 § Den som tar emot en hemlig handling i informationssäkerhetsklass Hemlig/Confidential eller högre ska kvittera på ett särskilt kvitto som utfärdas i två exemplar. Mottagaren behåller det ena kvittot och expeditionen det andra. Brutna sigill ska förstöras så att de inte går att återanvända.

11 § Registrator ska kvittera en inkommen kvalificerat hemlig handling (Hemlig/Top Secret) på det medföljande kvittot. Kvittot sänds tillbaka till avsändaren. Om försändelsen är skadad ska registratorn se till att distributören antecknar skadans art och omfattning. Registratorn anmäler skadan till avsändaren.

Delgivning av en hemlig uppgift till annan

12 § Om mottagaren av en hemlig handling med beteckningen Hemlig/Confidential eller högre låter någon annan ta del av handlingen ska personens namn samt datum antecknas på mottagarens kvitto. När handlingen återlämnas till expeditionen ska ansvarig tjänsteman anteckna på expeditionens kvitto att handlingen återlämnats.

Om även andra personer tagit del av handlingen ska deras namn anges på expeditionens kvitto.

Expeditionens kvitto ska sparas i minst 10 år när det gäller en hemlig handling i informationssäkerhetsklassen Hemlig/Confidential eller Hemlig/Secret. Kvittot ska sparas i minst 25 år när det gäller en kvalificerat hemlig handling, Hemlig/Top Secret.

13 § Om hemliga uppgifter, Hemlig/Confidential eller högre, lämnas muntligen eller visas för någon som inte tagit del av uppgifterna tidigare ska detta dokumenteras i ett särskilt protokoll. Av protokollet ska det framgå vilka uppgifter som lämnats, när och till vem de har lämnats. Protokollet ska förvaras vid expeditionen.

Registreringsmissiv

14 § För en kvalificerat hemlig handling, Hemlig/Top Secret, som expedieras utanför Pliktverket upprättar expeditionen ett registreringsmissiv och ett kvitto som skickas med handlingen till mottagaren. Expeditionen behåller ett bevakningskvitto. Bevakningskvittot ska förstöras när mottagaren kvitterat handlingen och återsänt sitt kvitto till Pliktverket. Det återsända kvittot ska sparas i minst 25 år.

Kopiering av och utdrag ur hemliga handlingar

15 § Kopia av eller utdrag ur hemliga handlingar, Hemlig/Confidential eller högre, får göras endast om det finns ett uppenbart behov. Verkschefen ska godkänna kopieringen eller utdrag av uppgifter som är kvalificerat hemliga. Vid kopiering eller utdrag ur en kvalificerat hemlig handling som inte upprättats vid Pliktverket ska registrator samråda med den myndighet som upprättat handlingen.

16 § När en hemlig handling, Hemlig/Confidential eller högre, kopieras eller ett utdrag görs ska detta antecknas av registratorn i det register eller system där handlingen är diarieförd. Av anteckningen ska det framgå till vem kopian eller utdraget har lämnats. När ett utdrag görs ska det framgå ur vilken handling utdraget är.

Förvaring av hemliga handlingar

17 § Expeditionen ska föra register över vilka som förvarar en hemlig handling i informationssäkerhetsklass Hemlig/Confidential eller högre. Registrator ska anteckna i registret om handlingar gallrats eller förkommit.

18 § Hemliga handlingar i informationssäkerhetsklass Hemlig/Confidential eller högre, ska om möjligt förvaras åtskilda från handlingar som inte innehåller hemliga uppgifter. Kvalificerat hemliga handlingar ska om möjligt förvaras åtskilda från andra hemliga handlingar.

19 § Hemliga handlingar i informationssäkerhetsklass Hemlig/Confidential eller högre, ska förvaras i värdeskåp eller säkerhetsskåp (SS 3492). Kvalificerat hemliga handlingar i informationssäkerhetsklass Hemlig/Top Secret ska förvaras i värdeskåp som är larmat eller placerat i larmat utrymme.

Flera personer får ha ett gemensamt förvaringsutrymme endast om de är behöriga att ta del av samma information och om avdelningschefen eller säkerhetsskyddschefen fattat ett samförvaringsbeslut.

20 § En hemlig handling i informationssäkerhetsklass Hemlig/Confidential eller högre får tillfälligt förvaras i handläggarens låsta tjänsterum. Detta förutsätter att ingen annan har nyckel eller kod till rummet, förutom den reservnyckel och kod som ska förvaras i särskilt kuvert vid expeditionen.

En kvalificerat hemlig handling ska hållas under ständig uppsikt när den inte förvaras i larmat värdeskåp.

21 § En hemlig handling i informationssäkerhetsklass Hemlig/Confidential eller högre får medföras utanför Pliktverkets lokaler endast efter skriftligt beslut av avdelningschefen. Handlingen ska då hållas under ständig uppsikt eller förvaras enligt samma säkerhetsbestämmelser som gäller inom myndighetens lokaler.

22 § När handläggaren inte längre behöver en hemlig handling i informations-säkerhetsklass Hemlig/Confidential eller högre för sin tjänst ska den återlämnas till expeditionen och arkiveras eller förstöras.

23 § En hemlig handling som har placerats i informationssäkerhetsklass Hemlig/Restricted ska förvaras inlåst eller i en lokal som endast den som är behörig att ta del av handlingen har tillträde till. Handlingen behöver inte kvitteras eller inventeras.

24 § Sigill, assuranstejp, plomberingstång och präglinganordning för sigillsvets ska förvaras på samma sätt som en hemlig handling. Detsamma gäller karbonpapper, karbonband, färgband, färgbandskassetter eller liknande materiel som använts vid arbete med hemliga uppgifter om uppgifterna kan ha lämnat spår i materialet.

Åtgärd då en hemlig uppgift kan ha röjts

25 § Om en hemlig uppgift kan ha röjts ska detta genast anmälas till säkerhetskyddschefen.

Inventering av hemliga handlingar

26 § En gång per år ska Pliktverkets hemliga handlingar i informationssäkerhetsklass Hemlig/Confidential eller Hemlig/Secret inventeras av en person som är anställd vid Pliktverket. Två anställda ska inventera handlingar i säkerhetsklass Hemlig/Top Secret. Protokoll ska föras och detta ska förvaras vid expeditionen. Arkiverade hemliga handlingar behöver inventeras endast om de är kvalificerat hemliga (Hemlig/Top Secret). Om en hemlig handling saknas vid inventeringen ska detta omedelbart anmälas till säkerhetsskyddschefen.

Förstöring av hemliga handlingar

27 § En hemlig handling i informationssäkerhetsklass Hemlig/Confidential eller högre ska förstöras i godkänd destruktör. När handlingen är förstörd ska det vara omöjligt att återskapa informationen med hjälp av restprodukterna. Disketter och bandkassetter får förstöras i centraldestruktörer eller specialdestruktörer. Hårddiskar kan förstöras genom t.ex. blästring av lagringsmediets yta eller genom nedsmältning. Märkningen av en dators ytterhölje får tas bort först sedan de hemliga uppgifterna avlägsnats ur datorn.

28 § Minst två av Pliktverkets anställda ska närvara samtidigt när en hemlig handling i informationssäkerhetsklass Hemlig/Confidential eller högre förstörs vid Pliktverket. Åtgärden ska dokumenteras på expeditionens kvitto eller i en särskild förstöringsrapport. Kvittot eller förstöringsrapporten ska dateras och undertecknas av samtliga närvarande och det ska framgå hur handlingen förstördes.

Kvittot eller förstöringsrapporten ska sparas i minst 10 år när det gäller hemliga handlingar i informationssäkerhetsklass Hemlig/Confidential och

Hemlig/Secret och minst 25 år när det gäller kvalificerat hemliga handlingar, Hemlig/Top Secret.

29 § Om en utomstående har fått uppdraget att förstöra en hemlig handling, ska minst en av Pliktverkets anställda närvara när handlingen förstörs. Minst två av Pliktverkets anställda ska närvara när en kvalificerat hemlig handling förstörs. Förstöringen ska dokumenteras i en särskild, daterad förstörings-rapport där det ska framgå hur förstöringen gått till. Pliktverkets anställda ska intyga att uppgifterna i rapporten är korrekta.

Förstörringsrapporten ska sparas i minst 10 år eller minst 25 år som anges i § 28.

30 § Förstöring av hemliga uppgifter i informationssäkerhetsklass Hemlig/Confidential eller högre som finns på datamedia, såsom disketter, hårddiskar och minneskort ska dokumenteras i en särskild liggare.

31 § Förstöring av karbonpapper, karbonband, färgband, färgbandskassetter och liknande materiel som använts vid framställning eller försändning av en hemlig handling behöver inte dokumenteras.

Distribution av hemliga handlingar

32 § Hemliga handlingar i informationssäkerhetsklass Hemlig/Confidential eller högre, ska sändas i förseglat emballage. Det ska vara omöjligt att ta del av innehållet utan att bryta förseglingen. En hemlig handling ska inneslutas i två kuvert inklusive emballaget och en kvalificerat hemlig handling i tre kuvert inklusive emballaget.

33 § Hemliga handlingar i informationssäkerhetsklass Hemlig/Confidential eller högre ska sändas som rekommenderad post och kvalificerat hemliga handlingar, Hemlig/Top Secret, som värdepost.

34 § Ett exemplar av daglistan på arkivpapper ska bifogas när en hemlig handling i informationssäkerhetsklass Hemlig/Confidential eller högre sänds mellan Pliktverkets enheter i form av utdata från Pliktverkets datasystem.

35 § En hemlig handling i informationssäkerhetsklass Hemlig/Confidential eller högre får sändas endast med distributör som är godkänd av Pliktverket. Säkerhetsskyddschefen eller den han utser ska skriftligt godkänna distributören.

Utrikesdepartementets kurirförbindelser ska anlitas när en hemlig handling ska sändas utomlands.

36 § Om hemliga uppgifter i informationssäkerhetsklass Hemlig/Confidential eller högre, ska sändas via teleförbindelse ska ett av Försvarmakten godkänt kryptosystem användas.

4 kap. Tillträdesbegränsning

1 § Med tillträdesbegränsning avses skydd mot att obehöriga får tillträde till platser där de kan få tillgång till uppgifter som omfattas av sekretess och rör rikets säkerhet eller där man bedriver verksamhet som har betydelse för rikets säkerhet.

Tillträdesskydd

2 § Säkerhetsskyddschefen svarar för bestämmelser om tillträdesskydd i Karolinen och när det gäller regionkontoren i samråd med regionkontorets säkerhetsansvarige.

Koder och nycklar

3 § Expeditionen ska föra en särskild förteckning över samtliga nycklar till utrymmen där hemliga handlingar i informationssäkerhetsklass Hemlig/Confidential eller högre förvaras. Av förteckningen ska det framgå vem som har en nyckel och när nyckeln överlämnades.

4 § Koden eller reservnyckeln till ett förvaringsutrymme för hemliga handlingar i informationssäkerhetsklass Hemlig/Confidential eller högre ska förvaras i ett förseglat emballage som måste brytas för att koden eller nyckeln ska kunna tas ut eller för att nyckelaxet ska kunna avläsas. Emballaget med koden eller nyckeln ska förvaras på samma sätt som den handling som förvaras i utrymmet.

5 § Den som tilldelas ett förvaringsutrymme för hemliga handlingar i informationssäkerhetsklass Hemlig/Confidential eller högre ska själv bestämma och ställa in koden till utrymmet. Koden ska alltid ställas om när någon övertar ett förvaringsutrymme från en annan person.

6 § Ingen annan än den som ansvarar för ett förvaringsutrymme med hemliga handlingar i informationssäkerhetsklass Hemlig/Confidential eller högre får öppna utrymmet om inte avdelningschefen skriftligt beslutar detta. Ytterligare en anställd ska närvara när utrymmet öppnas av någon annan än den som ansvarar för utrymmet. Av avdelningschefens beslut ska det framgå vem som får bevittna öppnandet.

När ett utrymme öppnats av någon annan än den som tilldelats det, ska detta dokumenteras i nyckel- eller kodförteckningen. Av anteckningen ska framgå om reservnyckel använts, vilken handling som tagits ur utrymmet och vem som tagit del av den. Anteckningen ska dateras och undertecknas såväl av den som öppnat utrymmet som av vittnet. Reservnyckel eller kod ska läggas i ett nytt emballage, som förseglas. Utrymmets innehavare ska underrättas snarast möjligt.

7 § Om en nyckel har förkommit, kan ha kopierats eller utnyttjats av någon obehörig ska detta omedelbart anmälas till säkerhetsskyddschefen. Detsamma gäller om en kod kan ha röjts eller utnyttjats av någon obehörig.

Säkerhetsskyddschefen ska omedelbart underrättas när ett inpasseringskort har förkommit eller om det kan antas att någon obehörig har använt kortet.

Återlämning av materiel och handlingar

8 § Den som slutar sin anställning ska återlämna kvitterade handlingar och utrustning till myndigheten. Detta gäller även inpasseringskort och aktiva kort.

9 § Den som ska vara borta från arbetsplatsen en längre tid ska till expeditionen överlämna nyckel till förvaringsutrymme med hemliga handlingar i informationssäkerhetsklass Hemlig/Confidential eller högre. Expeditionen ska förvara nyckeln på samma sätt som en reservnyckel.

5 kap. Säkerhetsprövning av egen personal

1 § Med säkerhetsprövning avses den prövning enligt säkerhetsskyddslagen som ska förebygga att personer som är opålitliga ur säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet.

Säkerhetsprövning genomförs av avdelningen för personalredovisning och verksamhetsstöd.

2 § Avdelningschefen ska en gång per år pröva vilka befattningar som ska vara placerade i säkerhetsklass. Motiverade förslag till förändringar ska anmälas till säkerhetsskyddschefen. Verkschefen beslutar om placering i säkerhetsklass 2 eller 3 efter föredragning av säkerhetsskyddschefen.

3 § Säkerhetsskyddschefen eller den han utser ska föra en förteckning över de befattningar som är placerade i säkerhetsklass.

4 § Avdelningen för personalredovisning och verksamhetsstöd ska göra en framställan till Rikspolisstyrelsen om registerkontroll av egen personal. Rikspolisstyrelsen meddelar närmare anvisningar om hur en sådan framställan ska vara utformad. Av anvisningarna framgår det också att en ny kontroll ska göras i vissa fall, till exempel när de personliga förhållandena ändras.

Om underlaget från Rikspolisstyrelsen innehåller uppgifter ur polisens register eller om det framkommit uppgifter som ger anledning till tvekan om den kontrollerade ska anställas eller inte, ska säkerhetsskyddschefen yttra sig innan beslut om anställning får tas.

5 § Resultatet av genomförd säkerhetsprövning ska dokumentera resultatet i enlighet med föreskrifterna i 38 § säkerhetsskyddsförordningen (1996: 633).

6 § Det åligger avdelningschefen att se till att skyddsåtgärder vidtas om en anställd kan antas innebära en säkerhetsrisk. Innan åtgärder vidtas ska säkerhetsskyddschefen och personaldirektören få tillfälle att yttra sig.

7 § Chefen för avdelningen för personalredovisning och verksamhetsstöd ska särskilt bestämma vilka personer som får handlägga ärenden som innehåller uppgifter ur polisregister om den egna personalen. Säkerhetsskyddschefen är anmäld kontaktperson till Säkerhetspolisen (SÄPO).

6 kap. Utbildning i säkerhetsskydd

1 § Säkerhetsskyddschefen ansvarar för att Pliktverket har en plan för utbildning om säkerhetsskydd samt en förteckning över de anställda som genomgått utbildningen.

7 kap. Kontroll av säkerhetsskyddet

1 § Pliktverkets säkerhetsskyddschef ansvarar för kontrollen av säkerhetsskyddet.

2 § Vid varje regionkontor ska det finnas en säkerhetsansvarig tjänsteman. Säkerhetsskyddschefen bestämmer i samråd med avdelningschefen för regionkontoret den säkerhetsansvariges uppgifter och ansvar. Uppgifter och ansvar kan införas i den lokala säkerhetsplanen.

3 § Säkerhetsskyddet ska kontrolleras kontinuerligt. Kontrollen ska säkerställa att bestämmelserna om säkerhetsskydd följs och att skyddsnivån är anpassad till den aktuella hotbilden. Säkerhetsskyddschefen ansvarar direkt under verkschefen för kontrollerna, med stöd av de säkerhetsansvariga vid regionkontoren.

4 § Säkerhetsskyddschefen ska göra säkerhetskontroller vid samtliga avdelningar där hemliga uppgifter förekommer eller kan förekomma. Kontrollerna ska följa en fastställd plan och protokollföras.

5 § Regionkontorens säkerhetsansvariga ska göra begränsade säkerhetskontroller vid den egna avdelningen efter anvisningar från säkerhetsskyddschefen.

6 § Fel eller brister i säkerhetsskyddet vid regionkontoren ska anmälas till den säkerhetsansvarige, som underrättar säkerhetsskyddschefen. Vid avdelningarna i Karlstad ska anmälan göras till säkerhetsskyddschefen. Anmälan kan vara muntlig men ska alltid antecknas av mottagaren.

7 § Fel eller brister i säkerhetsskyddet ska åtgärdas snarast möjligt. Om en anmälan inte leder till någon åtgärd ska detta antecknas av säkerhetsskyddschefen på den handling där anmälan dokumenterats.

8 § Säkerhetsskyddschefen svarar för att en säkerhetsanalys enligt 5 § säkerhetsskyddsförordningen görs en gång varje år och att analysresultatet dokumenteras.

8 kap. IT-säkerhet

1 § För IT-säkerhet inom informationssäkerheten finns en kompletterande intern bestämmelse.

9 kap. Signalskydd

1 § I Pliktverkets signalskyddsplan finns kompletterande anvisningar om signalskyddstjänst.

10 kap. Säkerhetsskyddad upphandling med säkerhetsskyddsavtal

1 § En säkerhetsanalys ska ligga till grund för planerade och löpande säkerhetsskyddade upphandlingar. Säkerhetsskyddschefen ansvarar för dessa analyser. Vid behov ska säkerhetsskyddsavtal tecknas.

2 § Säkerhetsskyddschefen eller den han har utsett är behörig att teckna säkerhetsskyddsavtal och ska delta i de förhandlingar som föregår avtalet.

3 § Inför en säkerhetsskyddad upphandling ska samråd alltid ske med avdelningen för personalredovisning och verksamhetsstöd och med säkerhetsskyddschefen.

4 § Vid säkerhetsskyddad upphandling ska avdelningen för personalredovisning och verksamhetsstöd genomföra säkerhetsprövning i samråd med säkerhetsskyddschefen.

Dessa bestämmelser träder i kraft den 1 november 2008 och samtidigt upphävs Pliktverkets interna bestämmelser (PIB 2006:10) om säkerhetsskydd.

BIRGITTA ÅGREN

Kjell Kastman