

Pliktverkets interna bestämmelser



Pliktverkets interna bestämmelser om IT-säkerhet

PIB 2008:10

beslutade den 14 oktober 2008.

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

1 kap. Grundläggande bestämmelser

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

2 § Dessa bestämmelser gäller säkerhet vid planering, utveckling, anskaffning och avveckling samt vid drift, ändring och annan användning av informationstekniska system (IT-system) inom Pliktverket.

2 kap. Tillsyn och ansvar

1 § Säkerhetsskyddschefen ska kontinuerligt kontrollera att dessa bestämmelser följs och att föreskrifterna tillämpas.

2 § Säkerhetsskyddschefen kan besluta om tillämpningen av dessa bestämmelser.

3 § Datorbearbetad information som innehåller eller kan innehålla hemliga uppgifter ska skyddas som hemlig uppgift enligt Försvarmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd.

4 § Vid inloggning i Pliktverkets IT-system ska inloggningsbilden om möjligt föregås av en bild där det framgår att endast den som är behörig får logga in i systemet.

5 § Säkerhetsskyddschefen har till sin hjälp en befattningshavare vid avdelningen för information och teknik som ansvarar för IT-säkerheten. Vid varje regionkontor ska det finnas en säkerhetsansvarig befattningshavare.

3 kap. Definitioner

1 § 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.
- *arbetsstation*: persondator som är ansluten till det lokala nätverket inom Pliktverkets område för tillträdesskydd.
- *säkerhetsloggning*: registrering av händelser i systemet som är av betydelse för säkerheten.

4 kap. Datakommunikation

1 § Datanät som är avsett för överföring av hemliga uppgifter får inte, vare sig fysiskt eller logiskt, kopplas ihop med ett datanät som inte är avsett för detta.

2 § Databärande medier får användas vid överföring av information mellan olika datanät om nödvändiga åtgärder har vidtagits för att förhindra spridning av skadliga program (datavirus).

3 § Utrustning för trådlös överföring får inte anslutas till Pliktverkets lokala nätverk eller bärbara datorer.

5 kap. Utveckling och anskaffning

1 § När nya IT-system införs ska de uppgifter dokumenteras som är av betydelse för säkerheten i systemet.

2 § Utveckling av samt prov och försök med ett IT-system får ske endast i en miljö som är skild från ordinarie driftmiljö. IT-säkerhetschefen får göra avsteg från denna bestämmelse efter samråd med säkerhetsskyddschefen.

6 kap. Godkännande från säkerhetssynpunkt

1 § Innan ett IT-system sätts i drift ska verkschefen godkänna säkerheten. Verkschefens beslut ska dokumenteras.

7 kap. Utnyttjande av IT-system.

1 § Innan en anställd får behörighet att utnyttja ett system ska den systemansvariga se till att personen kan hantera systemet på ett säkert sätt.

2 § Endast programvaror som godkänts av IT-säkerhetschefen får installeras i verkets IT-system. En förteckning över godkända programvaror ska finnas hos IT-säkerhetschefen.

8 kap. Behörighetskontroll

1 § Koder och kort som ger behörighet till ett IT-system är personliga och får inte visas eller lämnas till andra.

2 § IT-system som innehåller hemliga uppgifter ska vara konstruerade på ett sådant sätt att det krävs kod, eller kort och kod, för att få tillgång till uppgifterna.

3 § Kod och kort ska hanteras som en hemlig uppgift om koden eller kortet ger behörighet till ett IT-system som innehåller hemliga uppgifter.

9 kap. Skydd av arbetsstationer anslutna till det lokala nätverket

1 § Arbetsstationer som är anslutna till Pliktverkets lokala nätverk ska vara försedda med inloggningsfunktioner i form av användarnamn och lösenord.

2 § Arbetsstationer anslutna till Pliktverkets lokala nätverk får inte vara placerade utanför området för Pliktverkets tillträdesskydd utom vid tillfällig verksamhet utanför Pliktverkets lokaler. Vid sådan tillfällig verksamhet ska åtgärder vidtas och instruktioner utfärdas som innebär att säkerhetsskyddet når samma nivå som inom området för Pliktverkets tillträdesskydd.

3 § Inloggade arbetsstationer får inte lämnas obevakade.

10 kap. Användning av bärbara persondatorer och handdatorer

1 § Bärbara persondatorer bör vara försedda med en krypteringsfunktion.

2 § Bärbara persondatorer eller handdatorer får inte anslutas till Pliktverkets lokala nätverk. Chefen för avdelningen för planering och urval kan besluta om undantag för bärbara persondatorer som tillhör Pliktverket och som används enbart vid utflyttad mönstring. Innan anslutning ska datorerna kontrolleras så att de inte innehåller skadliga program (datavirus).

11 kap. Förhindra spridning av skadliga program (datavirus)

1 § Pliktverkets persondatorer med egna lagringsmedia ska om möjligt vara försedda med program som förhindrar spridning av skadliga program (datavirus).

2 § En särskild anvisad arbetsstation ska användas när data importeras eller exporteras via Pliktverkets lokala nätverk. Filer eller medier ska viruskontrolleras innan data får importeras eller exporteras.

3 § En arbetsstation avsedd för viruskontroll ska finnas vid avdelning för information och teknik samt på varje regionkontor. Arbetsstationen bör inte vara ansluten till ett nätverk.

4 § Den som gör viruskontrollerna ska dokumentera dem i en förteckning. Förteckningen ska visa när kontrollen är gjord, beställarens namn, från vilket media och mapp något flyttas, till vilken mapp och vem som har upprättat databäraren.

Det ska även anges vem som utfört viruskontrollen och datum när den är utförd. Om virus påträffats ska den som gjort kontrollen omedelbart anmäla detta till närmaste chef med uppgift om virusnamn. Databäraren ska makuleras efter utredning.

Om databäraren inte innehåller något virus och den enskilde handläggaren har fått tillbaka dokumentet bör databäraren sparas i högst 30 dagar hos den som gjort viruskontrollen. Därefter ska databäraren återlämnas, återanvändas eller makuleras.

5 § Endast arbetsstationer som anges i 2-3 § får användas för hantering av datamedia (diskett, cd, dvd eller USB-minne). Undantag gäller för arbete som utförs vid IT-utveckling -teknik och -drift samt persondator som enbart är ansluten till internet.

6 § Till kommunikationsportarna får endast utrustning som är godkänd av avdelningschef och IT-säkerhetschefen anslutas. Modem för telekommunikation får inte anslutas.

7 § Vid avdelning för information och teknik ska det finnas en tjänsteman med särskild kompetens inom området skydd mot skadliga program (datavirus). Denne ansvarar för uppdatering av skydd mot skadliga program (antivirusprogram).

12 kap. Säkerhetsloggning

1 § En säkerhetslogg får omfatta användaridentitet, datum och tidpunkt för på- och avloggning, registrering av lyckade och misslyckade försök till systemåtkomst, registrering av lyckade och misslyckade försök till åtkomst av data och andra resurser, om möjligt terminalidentitet och placering.

2 § Den systemansvariga ansvarar för att användare av ett IT-system informeras om att säkerhetsloggning sker.

3 § Säkerhetsskyddschefen har rätt att kontrollera loggarna.

BIRGITTA ÅGREN

Kjell Kastman