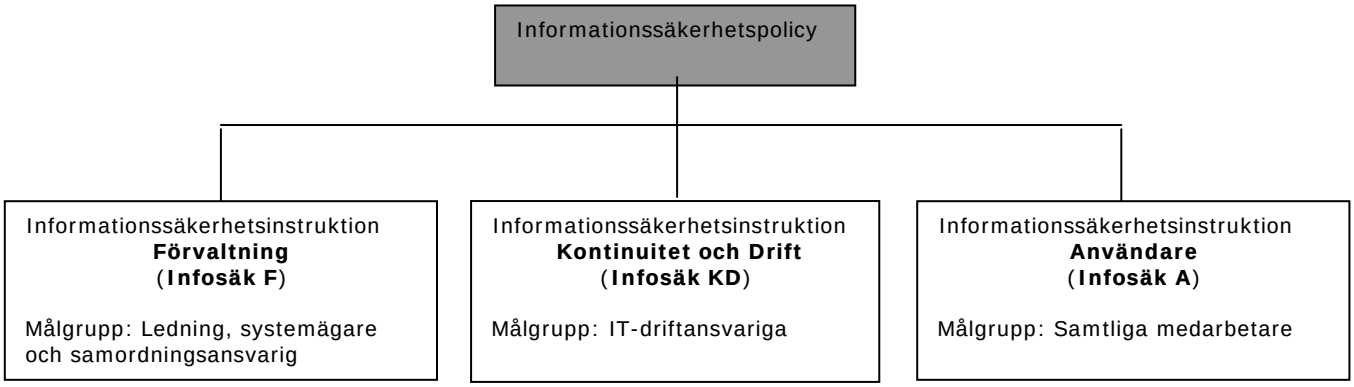
Informationssäkerhetspolicy

Informationssäkerhet är den del i organisationens lednings- och kvalitetsprocess som avser hantering av verksamhetens information. Informationssäkerhetspolicyn och särskilda informationssäkerhetsinstruktioner styr myndighetens informationssäkerhetsarbete.

1 Policyns roll i informationssäkerhetsarbetet



Informationssäkerhetspolicyn redovisar ledningens viljeinriktning och mål för informationssäkerhetsarbetet. Policyn konkretiseras i informationssäkerhetsinstruktioner.

2 Allmänt om informationssäkerhet

Information är en av våra viktigaste tillgångar och hanteringen av den är en viktig del i arbetet med myndighetens risk- och sårbarhetsanalys.

Utgångspunkter i vårt arbete med informationssäkerhet är:

- Lagar, förordningar och föreskrifter
- Våra egna krav
- Avtal

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationssäkerheten omfattar myndighetens informationstillgångar utan undantag. Med informationssäkerhet avses:

- att rätt information är tillgänglig för rätt person när den behövs och på ett spårbart sätt
- att informationen är och förblir riktig

Informationssäkerheten är en integrerad del av vår verksamhet. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett

ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till säkerhetsarbetet.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgångar.

Alla delar inom myndigheten är bundna av denna informationssäkerhetspolicy vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna.

Den som använder våra informationstillgångar på ett sätt som strider mot denna policy kan bli föremål för disciplinära åtgärder

3 Mål

För vårt informationssäkerhetsarbete ska gälla att:

- all personal har kunskap om gällande informationssäkerhetsregler
- att informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man
- ingångna avtal är kända och följs
- krishanteringsförmågan upprätthålls
- alla investeringar både i form av information och teknisk utrustning har skydd i tillräcklig grad
- det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- hotbilden för varje enskilt informationssystem som är av vikt för vår verksamhet analyseras fortlöpande
- händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs
- årliga mål för arbetet beslutas i och framgår av verksamhetsplaneringen. För de årliga målen anges:
    - vad som ska göras under året och hur
    - tidplan
    - behov av personella och ekonomiska resurser
    - när och hur uppföljning, utvärdering och avrapportering ska ske
    - när och hur våra medarbetare ska informeras och utbildas.

4 Roller och ansvar

Generaldirektören har det övergripande ansvaret för informationssäkerheten och utser systemägare för respektive informationssystem.

Informationssäkerhetssamordnaren utses av och är direkt underställd generaldirektören samt har det operativa ansvaret för samordning av informationssäkerhetsarbetet.

Systemägaren är den som har ansvaret för den verksamhet som aktuellt informationssystem stödjer.

Systemförvaltarna utses av respektive systemägare och ansvarar för den dagliga användningen av informationssystemen.

IT-chefen ansvarar för att uppfylla myndighetens kontinuitetsplan (Infosäk KD) för IT-stödet.

Beskrivning av roller och ansvar framgår av Informationssäkerhetsinstruktion Förvaltning (Infosäk F)

5 Generella krav

5.1 Myndighetens informationssystem

Samtliga informationssystem ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är systemägare. Alla informationssystem ska minst klara den basnivå för informationssäkerhet som myndigheten rekommenderar (BITS).

Vissa informationssystem är en förutsättning för att kunna bedriva vår verksamhet. För dessa ska en riskanalys upprättas med stöd av myndighetens verktyg för analys av informationssäkerhet (BITS Plus). Analysen ska utgöra underlag för driftgodkännande.

5.2 Informationssäkerhetsutbildning

All personal ska regelbundet få den utbildning som behövs för att informationssäkerheten ska upprätthållas.

5.3 Informationsklassning

Information som hanteras på myndigheten ska klassificeras med avseende på sekretess, riktighet och tillgänglighet enligt myndighetens klassningsmodell.

5.4 Distansarbete

För att personalen ska kunna arbeta effektivt ska möjlighet finnas att arbeta mobilt eller stationärt på distans. Förutsättningar och restriktioner för detta ska dokumenteras.

5.5 Användning av Internet

Vid användning av Internet exponeras myndighetens namn. Bland annat av detta skäl är det därför av vikt att lägga restriktioner på vilka hemsidor som får besökas. Hemsidor med exempelvis rasistiskt, våldsinriktat eller sexuellt innehåll får inte besökas. Undantag från detta kan beviljas av chef om informationen på sådana sidor kan ha relevans för arbetsuppgifterna.

5.6 Elektronisk post

Sekretessbelagd information får inte skickas via e-post.

5.7 Kontinuitetsplanering

Kontinuitetsplaneringen är av central betydelse för att bedriva verksamheten på en acceptabel nivå under såväl normala förhållanden som vid extraordinära händelser. En kontinuitetsplan ska finnas för driften av IT-verksamheten baserad på de olika informationssystemens samlade krav och vara integrerade med ORGANISATION X:s gemensamma kontinuitetsplan.

6 Revidering och uppföljning

Uppföljning är en viktig del i informationssäkerhetsarbetet för att bevaka att:

- beslutade åtgärder är genomförda
- årliga mål är uppfyllda
- regler följs
- att policy, säkerhetsinstruktioner och riskanalyser vid behov revideras.