Torsås kommun

2009-05-04

Informationssäkerhetspolicy

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

1 Policyns roll i informationssäkerhetsarbetet

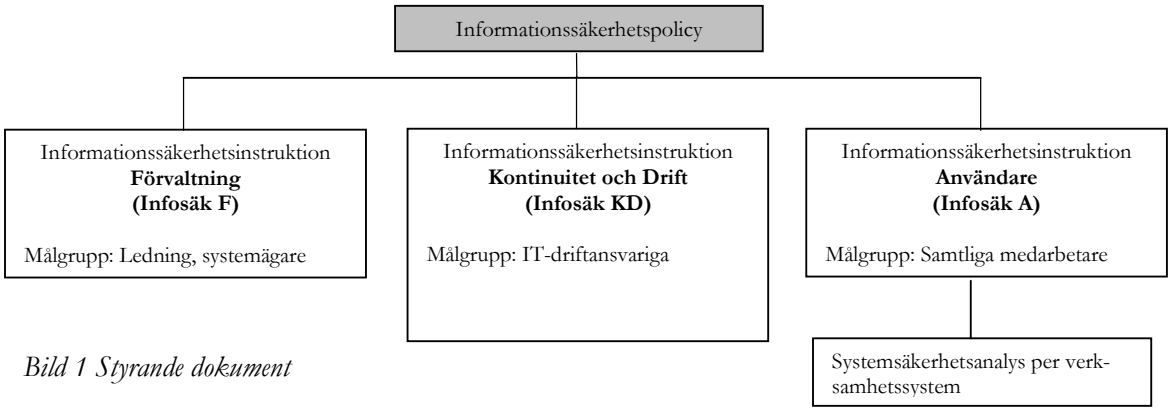

Bild 1 Styrande dokument

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 kommunens 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 kommunens 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 kommun 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.
- Samtliga IT är identifierade och förtecknade samt systemägare för dessa är utsedda av kommunfullmäktige.
- Kommunfullmäktige har fattat beslut om vilka system som är samhällsviktiga.
- De samhällsviktiga IT-systemen har en upprättad systemsäkerhetsanalys.

4 Organisation, roller och ansvar

4.1 Övergripande ansvar

Det övergripande ansvaret för säkerheten i organisationens IT-verksamhet vilar på kommunstyrelsen.

4.2 Roller och ansvar

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

5 Revidering och uppföljning

Uppföljning är en viktig del i IT-säkerhetsarbetet.
Uppföljningen ska bevaka:

- Att beslutade åtgärder är genomförda.
- Årliga mål är uppfyllda.
- Att riktlinjer följs.
- Att systemsäkerhetsplaner och policydokument vid behov revideras.

Informationssäkerhetspolicy, Säkerhetsinstruktioner och *Systemsäkerhetsplaner* ska löpande följas upp och vid behov revideras.