SKÖVDE

Program

Policy

Plan

» Riktlinjer

Regler

# Riktlinjer för informations-säkerhet i Skövde kommun

Beslutad av kommunstyrelsen
6 december 2010, § 214. Dnr KS10/0257

# Innehåll

1 Policyns roll i informationssäkerhetsarbetet ..... 3
2 Allmänt om informationssäkerhet ..... 4
3 Mål ..... 4
4 Organisation, roller och ansvar ..... 5
5 Generella krav ..... 5
5.1 Kommunens informationssystem ..... 5
5.2 Kontinuitetsplanering ..... 6
6 Revidering och uppföljning ..... 6

**Dokumenttyp**: Riktlinjer

**Dokumentet gäller för**: Samtliga nämnder och sektorer

**Diarienummer**: KS10/0257

**Reviderad**: ej reviderad

**Giltighetstid**: Tillsvidare

**Tidpunkt för aktualitetsprövning**: En gång per mandatperiod

**Dokumentansvarig**: Chef avdelning IT och verksamhetsutveckling

**Andra tillhörande dokument**: -

Riktlinje för informationssäkerhet i Skövde kommun motsvarar *Informationssäkerhetspolicy* enligt BITS såsom Myndigheten för samhällsskydd och beredskap föreskriver. I dokumentet kommer fortsättningsvis termen *Informationssäkerhetspolicy* att användas.

# 1 Policyns roll i informationssäkerhetsarbetet

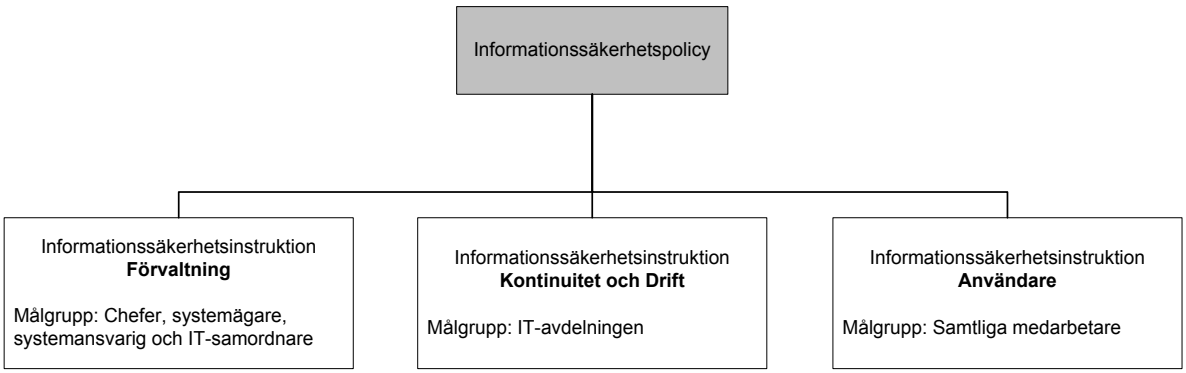
Informationssäkerhet är den del i organisationens lednings- och kvalitetsprocess som avser hantering av verksamhetens information. Informationssäkerhetspolicyn och särskilda informationssäkerhetsinstruktioner styr kommunens informationssäkerhetsarbete.

Denna Informationssäkerhetspolicy är en del av kommunens IT-verksamhet och redovisar ledningens viljeinriktning och stöd för informationssäkerhetsarbetet. Informationssäkerhetspolicyn syftar till att klarlägga:

- mål för informationssäkerhetsarbetet
- organisation, ansvar och roller inom informationssäkerhetsområdet
- krav

Policyn konkretiseras i Informationssäkerhetsinstruktionerna för Förvaltning, Kontinuitet och Drift samt Användare.

Styrande dokument:



# 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

Informationstillgångar avser all digital information. Informationssäkerheten omfattar kommunens informationstillgångar. 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 kommunen är bundna av denna informationssäkerhetspolicy vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna.

Det är inte tillåtet att använda kommunens informationstillgångar på ett sätt som strider mot denna policy.

Informationssäkerhetspolicyn fastställs av kommunstyrelsen. Informationssäkerhetsinstruktionerna fastställs av kommundirektören.

# 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
- 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 verksamheten analyseras fortlöpande

- årliga mål för arbetet beslutas i och framgår av verksamhetsplaneringen

# 4 Organisation, roller och ansvar

*Kommundirektören* har det övergripande ansvaret för informationssäkerheten.

*Informationssäkerhetssamordnaren* utses av IT-chef och har det operativa ansvaret för samordning av informationssäkerhetsarbetet.

*Systemägaren* utses av berörd förvaltningschef och är normalt den som har ansvar för den verksamhet som aktuellt informationssystem stödjer.

*Systemansvarig* utses av systemägaren och ansvarar för den dagliga användningen av informationssystemen.

IT-chefen ansvarar för att uppfylla kommunens kontinuitetsplan för IT-stödet.

Beskrivning av roller och ansvar framgår av Informationssäkerhetsinstruktion Förvaltning.

Organisation, roller och fördelning av ansvar ska säkerställa att ett IT-system kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla Informationssäkerhetspolicyns mål. Detta innebär att ett IT-system med alla dess delar är en resurs i en verksamhet på samma sätt som personal, lokaler, utrustning med mera.

Den interna organisationen för informationssäkerhetsarbetet framgår av Informations-säkerhetsinstruktion Förvaltning.

# 5 Generella krav

## 5.1 Kommunens 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 kommunen rekommenderar (BITS).

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

## 5.2 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 Skövde kommuns gemensamma kontinuitetsplan.

# 6 Revidering och uppföljning

Uppföljning är en viktig del i informationssäkerhetsarbetet.

Uppföljningen ska bevaka:

- att beslutade åtgärder är genomförda
- årliga mål är uppfyllda
- att instruktioner följs
- att policies, säkerhetsinstruktioner och riskanalyser vid behov revideras