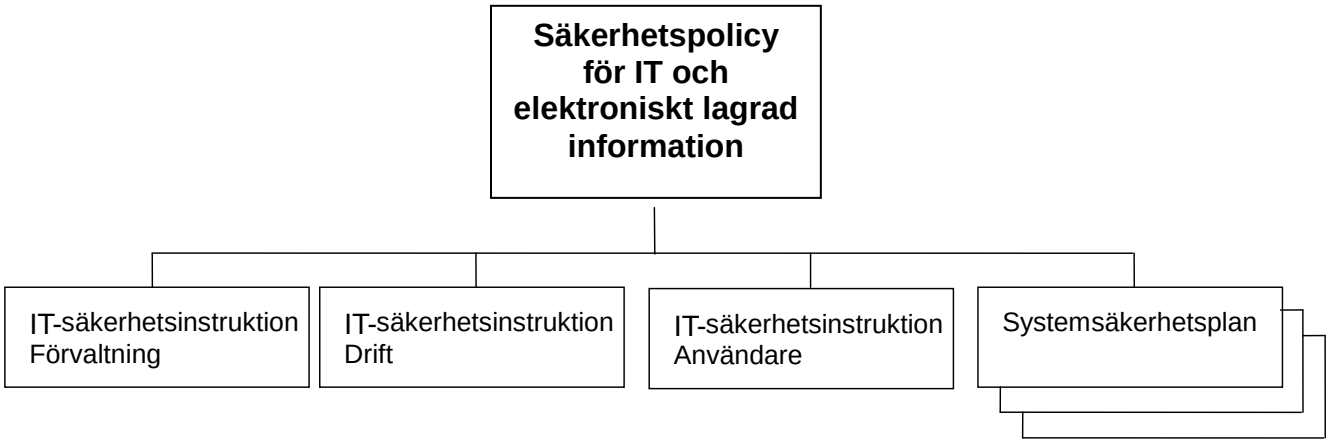
SVENLJUNGA KOMMUN	**Styrdokument**
	Dokumenttyp: Policy
	Beslutat av: Kommunfullmäktige
	Fastställelsedatum: 2006-03-27 § 29
	Ansvarig: IT-chef
	Revideras: Vid behov
	Följas upp:

SÄKERHETSPOLICY FÖR IT OCH ELEKTRONISKT LAGRAD INFORMATION

(I dokumentet omnämnd som IT-säkerhetspolicy)



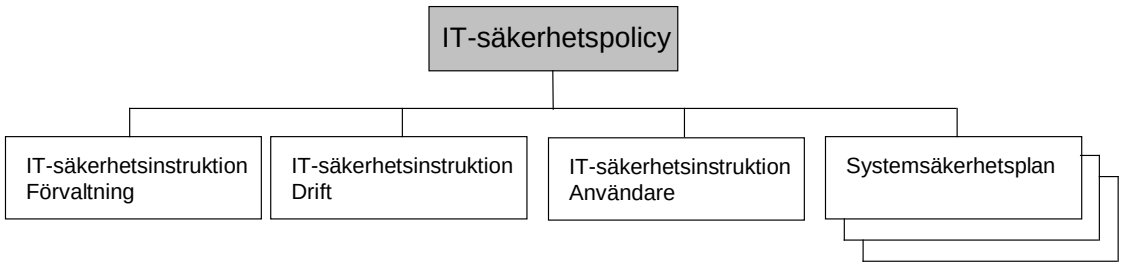
1 INLEDNING

IT-säkerhet är en del i organisationens lednings- och kvalitetsprocess som ska bidra till att IT-systemen kan användas på avsett sätt och med avsedd funktionalitet. Krisberedskaps-myndighetens (KBM) rekommendationer om basnivå för IT-säkerhet (BITS) ska gälla som ramverk för IT-säkerhetsarbetet.

IT-säkerhetspolicyn är ett styrdokument för Svenljunga kommuns IT-användning och fastställs av Kommunfullmäktige. IT-säkerhetspolicyn är underordnad IT-policyn. IT-säkerhetspolicyn redovisar Kommunsfullmäktiges viljeinriktning och stöd för IT-säkerhetsarbetet samt syftar till att klarlägga:

- mål för IT-säkerhetsarbetet
- organisation, ansvar och roller inom IT-säkerhetsområdet
- riktlinjer för områden av särskild betydelse.

Policyn konkretiseras i de tre IT-säkerhetsinstruktionerna: Förvaltning, Drift och Användare samt i Systemsäkerhetsplaner. IT-säkerhetsinstruktionerna fastställs av IT-styrgruppen.



Figur 1. Styrande dokument

2 MÅL FÖR IT-SÄKERHETSARBETET

2.1 Långsiktiga mål

För organisationens IT-säkerhetsarbete ska gälla att:

- Lagar och föreskrifter följs
- Verksamhetsutvecklingsarbetet stöds
- Krishanteringsförmågan säkerställs
- Det förebygger oväntade händelser i IT-systemen som kan leda till negativa konsekvenser
- Säkra en effektiv informationsförsörjning som bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man
- Investeringar som görs och gjorts både i form av information (data) och teknisk utrustning skyddas i tillräcklig grad
- Informationen (data) ses som en tillgång och skyddas i paritet med dess värde
- All personal, som använder IT som ett arbetsredskap, ges kunskap om gällande IT-säkerhetsregler
- Det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- Hotbilden för varje enskilt samhällsviktig IT-system analyseras fortlöpande

De långsiktiga målen ska säkerställa att organisationen kan tillhandahålla relevant information som:

- Endast delges behöriga personer och kan levereras vid rätt tidpunkt och till skäliga kostnader
- Är riktig, komplett och aktuell
- Efterfrågas och som organisationen har ett ansvar att tillhandahålla

2.2 Årliga mål

IT-säkerhetsarbetet ska bedrivas som en integrerad del av organisationens normala verksamhet. Årliga mål för arbetet ska därför beslutas och framgå i verksamhetens budgetplanering.

För de årliga målen bör anges:
- vad ska göras under året
- tidplan (när och hur, sluttidpunkt)
- resurser för arbetet (personella och ekonomiska)
- när och hur uppföljning, utvärdering och avrapportering ska ske
- när och hur organisationens medarbetare ska informeras och utbildas.

3 ORGANISATION, ROLLER OCH ANSVAR

3.1 Övergripande ansvar

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

3.2 Roller och ansvar

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 IT-säkerhetspolicyns mål. Detta innebär att ett IT-system med alla dess delar är en resurs i en verksamhet på samma sätt som personal, lokaler, kontorsmaterial mm.

Samtliga IT-system och datorprogram ska vara identifierade och förtecknade. Kommunledningsgruppen (tjänstemanna) utser systemägare för dessa. Organisationens IT-system ska klara den basnivå för IT-säkerhet som KBM:s rekommendationer beskriver. För de samhällsviktiga IT-systemen ska en systemsäkerhetsplan vara upprättad i enlighet med KBM:s IT-säkerhetsguide. Planen ska utgöra underlag för utsedd systemägares beslut om driftgodkännande.

Den interna organisationen för IT-säkerhetsarbetet, roller, fördelning av ansvar och arbetssätt framgår av IT-säkerhetsinstruktion: Förvaltning.

4 SÄRSKILDA RUTINER

Vissa områden inom området IT-säkerhet är av särskild betydelse för organisationens verksamhet. Av IT-säkerhetsinstruktionerna ska nedanstående områden och de särskilda riktlinjer, regler och rutiner som gäller för dessa framgå enligt följande:

- IT-säkerhetsinstruktion Förvaltning: Områdena Behörighetsadministration, behörighetskontroll, loggning och sårbarhet, distansarbete, drift- och förvaltning, tillträdesskydd, säkerhetskopiering och lagring, Avveckling av datamedia och datakommunikation.
- IT-säkerhetsinstruktion Användare; Områdena Informationsklassning, distansarbete, IT-incidenthantering, säkerhetskopiering och lagring samt e-post och användning av Internet.
- IT-säkerhetsinstruktion Drift: Områdena system- och driftdokumentationer, förvaring av datamedia, bemanning, tillträdes- och brandskydd, elförsörjning, regler för säkerhetskopiering och förvaring av datamedia.

5 REVIDERING OCH UPPFÖLJNING

Uppföljning är en viktig del i IT-säkerhetsarbetet.
Uppföljningen ska bevaka att:
- beslutade åtgärder är genomförda
- årliga mål är uppfyllda
- riktlinjer följs

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