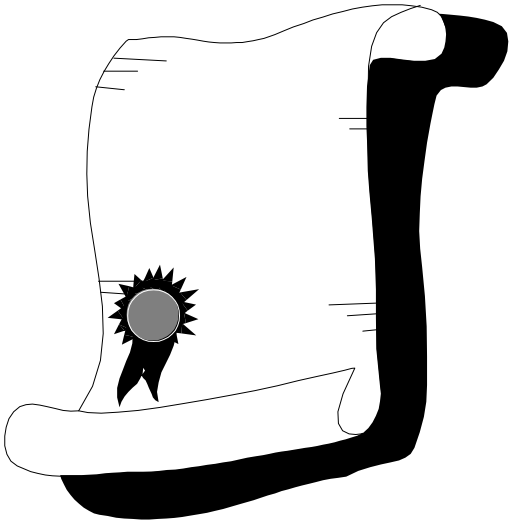
NORA KOMMUN

Nora kommun
IT-säkerhetspolicy



Antagen av kommunfullmäktige 2006 - -

Postadress
Tingshuset
713 30 NORA

Besökadress
Prästgatan 15
NORA

Telefon
0587-81 000

Telefax
0587-14 490

1 Inledning

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

Denna IT-säkerhetspolicy är en del av organisationens IT-verksamhet och redovisar ledningens viljeinriktning och stöd för IT-säkerhetsarbetet och syftar till att klarlägga:

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

Policyn konkretiseras i IT-säkerhetsinstruktionerna, Förvaltning, Drift och Användare samt i Systemsäkerhetsplaner.

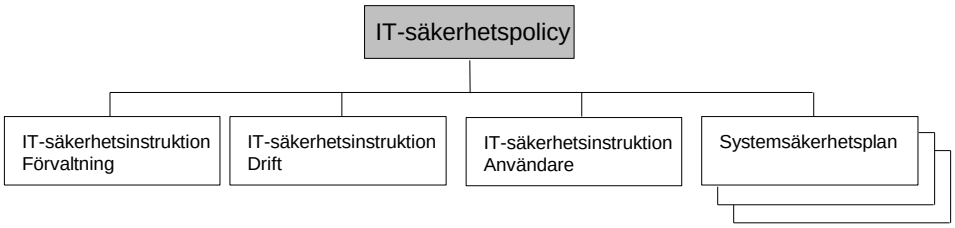


Bild 1 Styrande dokument

IT-säkerhetsinstruktionerna fastställs enligt bestämmelserna i organisationens arbetsordning.

2 Mål för IT-säkerhetsarbetet

2.1 Långsiktiga mål

För organisationens IT-säkerhetsarbete ska gälla att:

- lagar och föreskrifter följs
- det stöder utvecklingsarbetet
- krishanteringsförmågan säkerställs
- det förebygger oväntade händelser i IT-systemen som kan leda till negativa konsekvenser
- det säkrar en effektiv informationsförsörjning som bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man
- alla investeringar både i form av information (data) och teknisk utrustning skyddas i tillräcklig grad
- informationen ses som en tillgång och skyddas i paritet med dess värde
- all personal 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 av verksamhetsplaneringen.

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 kommunchefen.

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 ska vara identifierade och förtecknade och kommunchefen 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, 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
- att riktlinjer följs
- att systemsäkerhetsplaner och policydokument vid behov revideras

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