Malung-Sälens kommun

Informationssäkerhet

- Informationssäkerhetspolicy

Malung-Sälens kommun

Innehållsförteckning

1 Inledning 1
2 Mål för IT-sbäkerhetsarbetet 2
2.1 Långsiktiga mål *2*
2.2 Årliga mål *2*
3 Organisation, roller och ansvar 3
3.1 Övergripande ansvar *3*
3.2 Roller och ansvar *3*
4 Särskilda rutiner 4
5 Revidering och uppföljning 5

****
Fastställd av kommunstyrelsen den
Instruktionen kontrollerades senast den
Version
Ansvarig för dokumentet är kommunens informationssäkerhetssamordnare
Länk till dokumentet
****

Malung-Sälens kommun

1 Inledning

Informationssäkerhet är en del i kommunens lednings- och kvalitetsprocess som ska bidra till att ett informationssystem kan användas på avsett sätt och med avsedd funktionalitet. Krisberedskapsmyndighetens (KBM) rekommendationer om basnivå för informationssäkerhet ska gälla som ramverk för informationssäkerhetsarbetet.

Denna informationssäkerhetspolicy är en del av Malung-Sälens kommuns informationsverksamhet och redovisar kommunledningens viljeinriktning och stöd för informationssäkerhetsarbetet och syftar till att klarlägga:

- Mål för informationssäkerhetsarbetet
- Organisation, ansvar och roller inom informationssäkerhetsområdet
- Eventuella riktlinjer för områden av särskild betydelse

Policyn konkretiseras i informationssäkerhetsinstruktionerna Förvaltning, Kontinuitet & Drift och Användare samt i de enskilda systemens systemsäkerhetsplaner.

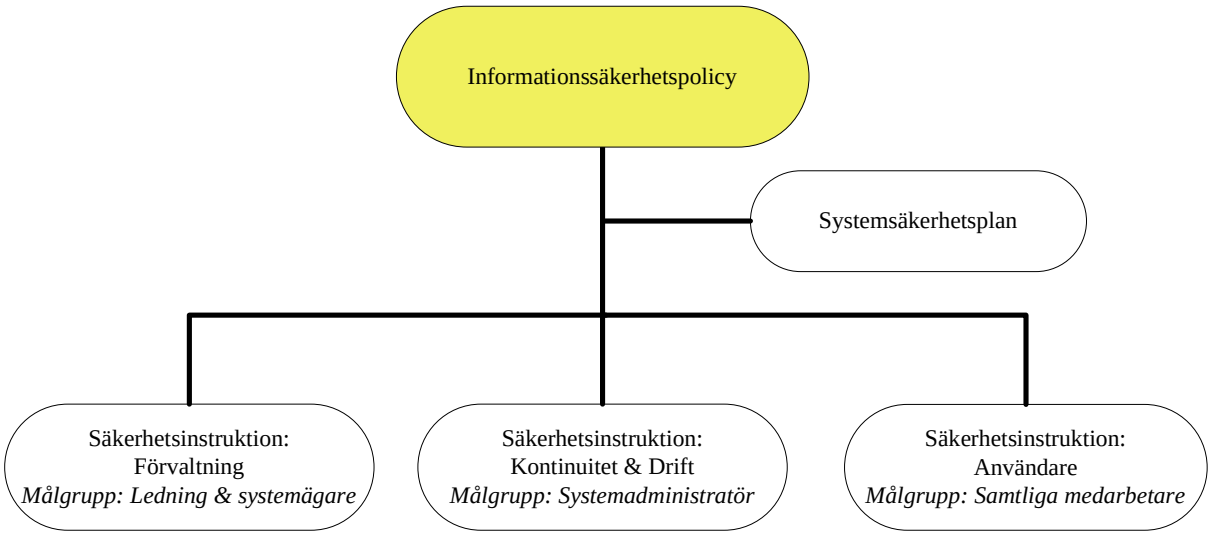

Bild 1 Styrande dokument

Informationssäkerhetsinstruktionerna fastställs enligt gällande beslutsordning i Malung-Sälens kommun.

Informationssäkerhetsarbetet i kommunen skall:

- Garantera hög kvalitet, effektivitet och tillförlitlighet i informationshanteringen
- Hindra och/eller minska effekterna av oönskade händelser
- Höja säkerhetsmedvetandet hos de anställda
- Skydda medborgarnas integritet samt bidra till att nyttjande av informationsteknik har deras förtroende

2 Mål för IT-säkerhetsarbetet

2.1 Långsiktiga mål

För kommunens informationssäkerhetsarbete ska gälla att:

- Lagar och föreskrifter följs
- Det stöder verksamheternas utvecklingsarbetet
- Krishanteringsförmågan säkerställs
- Det förebygger oväntade händelser i IT-systemen
- Det säkrar en effektiv informationsförsörjning som bidrar till ökat skydd och stöd för medarbetare, samverkande myndigheter/företag/privatpersoner och tredje man
- Alla IT-investeringar, både i form av information 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 informationssäkerhetsregler
- Det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- Hotbilden för varje enskilt samhällsviktigt informationssystem analyseras fortlöpande

De långsiktiga målen ska säkerställa att Malung-Sälens kommun 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

Informationssäkerhetsarbetet ska bedrivas som en integrerad del av organisationens normala verksamhet samt ingå i verksamhetsplanerna för kommunen, kommunstyrelsen och respektive nämnd. Årliga mål för arbetet ska därför fastställas i verksamhetsplanerna för i första hand kommunstyrelsen och respektive nämnd.

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 kommunens medarbetare ska informeras och utbildas

3 Organisation, roller och ansvar

3.1 Övergripande ansvar

Det övergripande ansvaret för säkerheten i kommunens 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 informationssäkerhetspolicyns mål. Detta innebär att ett IT-system med alla dess delar är en resurs i en verksamhet på samma sätt som personal, lokaler, kontorsmaterial m.m.

Samtliga informationssystem ska vara identifierade, förtecknade och det ska finnas av kommunstyrelsen utsedd systemägare för varje system. Kommunens system ska klara den basnivå för informationssäkerhet som KBM:s rekommendationer beskriver. För de samhällsviktiga informationssystemen ska en systemsäkerhetsplan vara upprättad i enlighet med KBM:s ”Basnivå för informationssäkerhet (BITS)”.

Den interna organisationen för informationssäkerhetsarbetet, roller, fördelning av ansvar och arbetssätt framgår av informationssäkerhetsinstruktionen Förvaltning.

4 Särskilda rutiner

Vissa områden inom området informationssäkerhet är av särskild betydelse för kommunens verksamhet. Av informationssäkerhetsinstruktionerna ska bl.a. nedanstående områden och de särskilda riktlinjer, regler och rutiner som gäller för dessa framgå enligt följande:

- Informationssäkerhetsinstruktion Förvaltning:

- Behörighetsadministration
- E-postadresser
- Loggning och spårbarhet
- Införande, utveckling och avveckling av IT-system
- Drift
- Incidenthantering
- Konsulters åtkomst till kommunens nätverk

- Informationssäkerhetsinstruktion Användare:

- Informationsklassning
- Användarens ansvar
- Behörighet och lösenord
- Arbetsplatsen
- Distansarbete
- E-post
- Internet
- Virus m.m.
- Avslutning av anställning
- Efterlevnad av instruktionen

- Informationssäkerhetsinstruktion Kontinuitet & Drift[1]:

- System- och driftdokumentationer
- Driftsgodkännande
- Kontinuitetsplanering
- Förvaring av datamedia
- Bemanning
- Tillträdes- och brandskydd
- Elförsörjning
- Regler för säkerhetskopiering och förvaring av datamedia.

[1] Avvaktar färdig instruktion Kontinuitet och Drift

5 Revidering och uppföljning

Uppföljning är en viktig del i informationssäkerhetsarbetet.

Uppföljningen ska bevaka

- att beslutade åtgärder är genomförda
- årliga mål är uppfyllda
- att riktlinjer följs
- att systemsäkerhetsplaner och policydokument vid behov revideras

Policy, informationssäkerhetsinstruktioner och systemsäkerhetsplaner ska löpande följas upp och vid behov revideras. Policy och informationssäkerhetsinstruktionerna ska dock minst revideras en gång per mandatperiod. Ansvaret för att revidering och löpande uppföljning görs ligger på informationssäkerhetssamordnare.