Policy för Informationssäkerhet (InfoSäkI P) för Arvika kommun

ARVIKA KOMMUN

Informationssäkerhet är en del i organisationens lednings- och kvalitetsprocess som ska bidra till att hantering av information sker på avsett sätt och med avsedd säkerhet.

Styrande dokument för informationssäkerhetsarbetet är:

Dokument	Innehåll
Informationssäkerhetspolicy (InfoSäk P)	Målgrupp: Ledning (mål och stöd för informationssäkerhetsarbetet)
Informationssäkerhetsinstruktion Systemförvaltning -IT (InfoSäkI SF)	Målgrupp: Ledning, systemägare och samordningsansvariga (Organisation, roller och ansvar)
Informationssäkerhetsinstruktion Kontinuitet och Drift -IT Del 1 (InfoSäkI KD-IT del 1)	Målgrupp: Ledning, systemägare och samordningsansvariga (Verksamhetens åtgärder vid olika typer av störningar samt del i den gemensamma kontinuitetsplanen)
Informationssäkerhetsinstruktion Kontinuitet och Drift -IT Del 2 (InfoSäkI KD-IT del 2)	Målgrupp: IT- ansvariga (Tekniska åtgärder och rutiner vid olika typer av störningar samt del i den gemensamma kontinuitetsplanen)
Informationssäkerhetsinstruktion Användare -IT (InfoSäkI A)	Målgrupp: Samtliga medarbetare (Användarnas ansvar)
Verksamhets- och nulägesanalys	Målgrupp: Ledning, systemägare (inventering av IT-stödet, klassificeringar och prioriteringar)
Systemsäkerhetsanalyser	Målgrupp: Systemägare (Egna IT-systems systemsäkerhetsanalyser, genomförda och återstående åtgärder)

Versionshantering InfoSäk P

Version	**Upprättad av**	**Datum**	**Status/Anmärkning**
Ver 1		2005-08-15	Dokumentet antaget av KS
Ver 1.1		2007-06-01	Revidering påbörjad
Ver 1.2		2008-01-20	Dokumentstruktur klar
Ver 1.3		2009-07-16	Prel vers klar
Ver 2.0		2009-09-22	Slutlig version klar
Ver 2.0			Godkänd av revisorer
Ver 2.0			Godkänd av ledningen

Relaterad information:

På Intranät eller hos dokumentägare:	**Dokumentägare:**
InfoSäk P	Säkerhetssamordnaren
InfoSäkI SF	-”-
InfoSäkI A	-”-
Larmlistor	-”-
Verksamhetsanalys	-”-
InfoSäkI KD-IT Del 1 och del 2	-”-
Systemsäkanalys Tekn. infrastruktur	IT-chef
Systemsäkanalys egen applikation	Systemägare berörd verksamhet

1 Syfte

Med information avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer. Utgångspunkter i vårt arbete med informationssäkerhet är:

• Verksamhetens krav
• Lagar, förordningar och föreskrifter

Syftet med denna policy är förebygga, förbereda, förhindra, upptäcka, hantera och ingripa så att vår information inte hanteras felaktigt i det dagliga arbetet och vid störningar av olika slag.

Informationssäkerhet är en integrerad del av verksamheten. Alla som hanterar information har ett ansvar att hålla sig själva informerade om och bidra till att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till informationssäkerhet. Alla medarbetare ska vara uppmärksamma på och rapportera händelser som kan påverka säkerheten för vår information.

Alla delar inom vår organisation är bunden till denna policy vilket medför att det inte finns utrymme att besluta om lokala policies eller regler som avviker.

2 Mål

Långsiktiga mål

För informationssäkerhetsarbetet ska gälla att:

- det ska säkerställa att rätt information är tillgänglig för rätt person i rätt tid och på ett spårbart sätt
- det stöder utvecklingsarbetet
- krishanteringsförmågan säkerställs
- det säkrar en effektiv och balanserad informationsförsörjning som bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man
- all personal har kunskap om gällande informationssäkerhetsregler
- det finns tillgång till en gemensam, säker och väl definierad teknisk infrastruktur och för extern och intern datakommunikation
- hotbilden för varje enskilt informationssystem som är av vikt för vår verksamhet ska analyseras regelbundet
- systemsäkerhetsanalyser av viktiga informationssystem ska prioriteras
- ingångna avtal är kända och följs

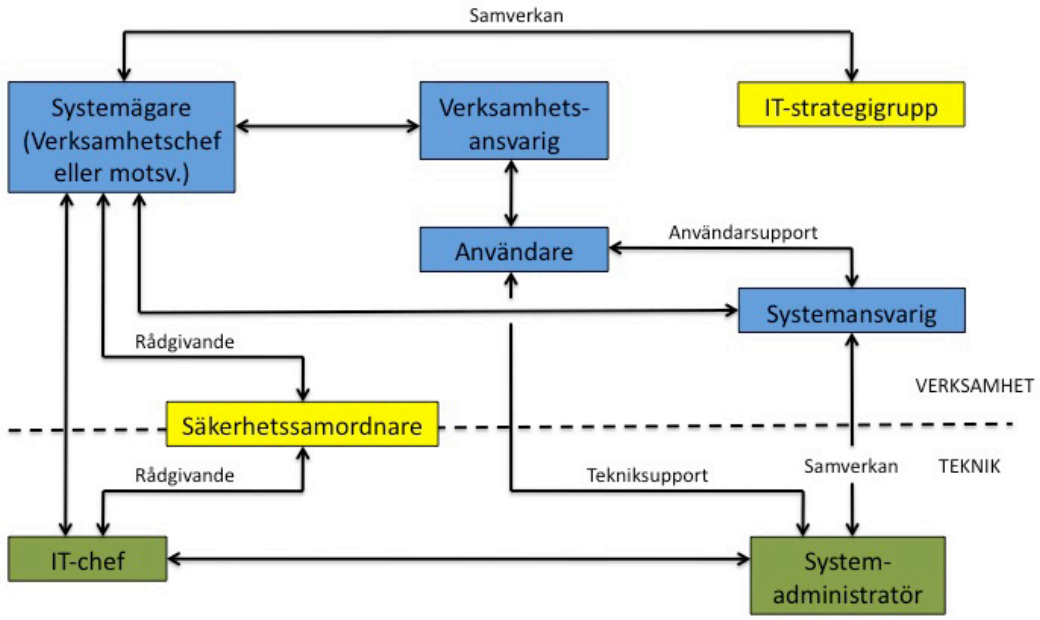
Årliga mål

Informationssäkerhetsarbetet ska bedrivas som en integrerad del av organisationens normala verksamhet. Årliga mål för det ska därför beslutas och framgå av verksamhetsplaneringen.

Av de årliga målen bör framgå:
• vad ska göras under året och varför
• tidplan (när och hur, sluttidpunkt)
• behov av resurser för arbetet (personella och ekonomiska)
• när och hur uppföljning, utvärdering och avrapportering ska ske
• när och hur medarbetare ska informeras och utbildas

3 Organisation, roller och ansvar

Organisation, roller och fördelning av ansvar ska bidra till att informationen kan administreras och hanteras på ett riktigt sätt. Detta innebär att ett informationssystem med alla dess delar är en resurs i en verksamhet på samma sätt som personal, lokaler, kontorsmaterial mm. Biträdande Kommundirektör har det övergripande ansvaret för informationssäkerheten. Beskrivning av ansvar och roller enligt bild nedan framgår av Informationssäkerhetsinstruktion Förvaltning (InfoSäkI SF)



4 Bild Ansvar och roller

4 Generella krav

Samtliga informationssystem ska vara identifierade och förtecknade och biträdande kommun direktör utser systemägare för dessa. Informationssystemen ska klara den basnivå för informationssäkerhet som KBM:s rekommendationer beskriver.

Vissa informationssystem är en förutsättning för oss att kunna bedriva vår verksamhet. Som underlag för beslut om vilka dessa är ska en verksamhetsanalys vara genomförd. För prioriterade system ska en systemsäkerhetsanalys genomföras/upprättas. Den ska utgöra underlag för utsedd systemägares beslut om driftgodkännande.

Vissa områden inom området informationssäkerhet är av särskild betydelse för vår verksamhet. Dessa områden är utbildning, informationsklassning, distansarbete, användning av Internet och e-post samt kontinuitetsplanering. För dessa områden ska särskilda regler finnas och framgå av informationssäkerhetsinstruktionerna.

Den som använder våra informationstillgångar på ett sätt som strider mot denna policy kan bli föremål för åtgärder från vår sida.

5 Revidering och uppföljning

Uppföljning är en viktig del i informationssäkerhetsarbetet och ska bevaka:
att beslutade åtgärder är genomförda, att årliga mål är uppfyllda, att regler följs och att systemsäkerhetsanalyser och policydokument vid behov revideras

Verksamhetsanalys, policy, informationssäkerhetsinstruktioner och systemsäkerhetsanalyser ska årligen följas upp och vid behov revideras.