RIKTLINJER FÖR

IT-SÄKERHET

Dokumenttyp Riktlinjer	Förvaltning KSF, stab
Ämnesområde IT	
Ägare/ansvarig IT-strateg	
Antagen av KS 2012-02-08 § 47	Dnr KS/2010:1056
Revisions datum	Giltig fr.o.m.
	Giltig t.o.m.

INNEHÅLLSFÖRTECKNING

Kommunstyrelsen beslutade 20xx-xx-xx § x att fastställa följande riktlinjer avseende IT-relaterad verksamhet inom Orust kommun.

Ersätter tidigare riktlinjer fastställda av kommunstyrelsen 2006-03-15 § 32

1 INLEDNING OCH BAKGRUND

IT-säkerhet är en allt viktigare del i kommunens lednings och kvalitetsprocess vilken ska leda till att samtliga IT-system kan användas på avsett sätt och med avsedd funktionalitet. Myndigheten för samhällsskydd och beredskap (MSB) rekommenderade basnivå för IT-säkerhet (BITS) ska gälla som ramverk för Orust kommun.

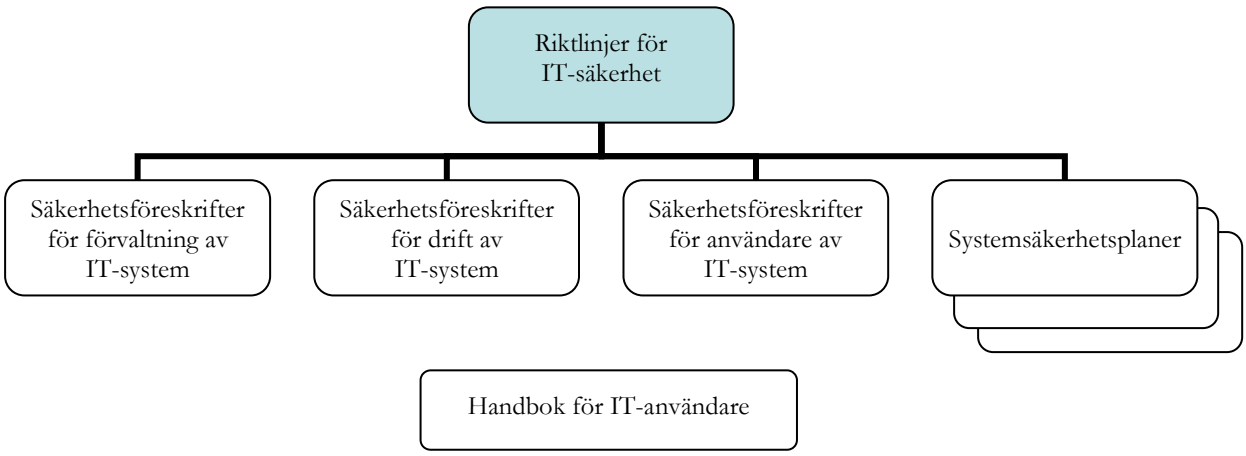
De av kommunfullmäktige antagna riktlinjerna för IT-säkerhet ska utgöra grunden för kommunens IT-verksamhet och redovisa kommunledningens viljeinriktning och stöd för IT-säkerhetsarbete samt syftar till att klarlägga:

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

Riktlinjerna för IT-säkerhet ska konkretiseras i IT-säkerhetsföreskrifterna för förvaltning, drift, användare och systemsäkerhetsplaner.

För att tydliggöra det ovan angivna för samtliga IT-användare inom Orust kommun ska en IT-handbok sammanställas och tillgängliggöras för samtliga användare.

1.1 Styrande dokument



IT-säkerhetsföreskrifterna och systemsäkerhetsplanerna ska fastställas enligt bestämmelserna i kommunens 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 IT-infrastruktur för extern och intern datakommunikation
- hotbilden för varje enskilt samhällsviktigt IT-system analyseras fortlöpande
- i varje systemsäkerhetsplan ska finnas en kontinuitetsplan. Dessa planer ska samordnas i en gemensam kontinuitetsplan.

De långsiktiga målen ska säkerställa att kommunens olika förvaltningar och verksamheter har tillgång till relevant information som:

- efterfrågas och som organisationen har ett ansvar att tillhandahålla
- endast är tillgänglig för behöriga personer och kan levereras vid rätt tidpunkt och till skäliga kostnader
- är riktig, komplett och aktuell

2.2 Årliga mål

IT-säkerhetsarbetet ska bedrivas som en integrerad del av kommunens 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 medarbetarna ska informeras och utbildas

3 ORGANISATION, ROLLER OCH ANSVAR

3.1 Övergripande ansvar

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

Samtliga IT-system ska vara identifierade och förtecknade och kommunstyrelsen utser systemägare för dessa. Kommunens IT-system ska klara den basnivå för IT-säkerhet (BITS) som Myndigheten för samhällsskydd och beredskaps (MSB) rekommendationer beskriver. För de särskilt samhällsviktiga IT-systemen ska en systemsäkerhetsplan vara upprättad i enlighet med Myndigheten för samhällsskydd och beredskaps (MSB) verktyg för informationssäkerhetsanalys. Planen ska utgöra underlag för utsedd systemägares beslut om driftgodkännande.

Den kommunala organisationen för IT-säkerhetsarbetet, roller, fördelning av ansvar och arbetssätt framgår av ”IT-säkerhetsföreskriften för förvaltning av IT-system”.

4 SÄRSKILDA RUTINER

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

IT-säkerhetsföreskrifter för förvaltning av IT-system: områdena behörighetsadministration, behörighetskontroll, loggning och spårbarhet, distansarbete, drift- och förvaltning, tillträdesskydd, säkerhetskopiering och lagring samt datakommunikation.

IT-säkerhetsföreskrifter för användare av IT-system: områdena informationsklassning och lagring, IT-säkerhet och kringutrustning, avveckling av datamedia, Internet och e-post samt incidenter, virus, stöld m.m.

IT-säkerhetsföreskrifter för drift av IT-system: områdena system- och driftdokumentationer, förvaring av datamedia, bemanning, tillträdes- och brandskydd, elförsörjning, regler för säkerhetskopiering och förvaring av datamedia.

5 REVIDERING OCH UPPFÖLJNING

5.1 Uppföljning är en viktig del i IT-säkerhetsarbetet

Genom regelbunden och kontinuerlig uppföljning ska bevakas

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