Bromölla kommun

KOMMUNAL FÖRFATTNINGSSAMLING **Nr 005.6**

Antagen/Senast ändrad	**Gäller från**	**Dnr**
Kf 2013-09-30 § 151	2013-10-01	2013/320

RIKTLINJER FÖR INFORMATIONSSÄKERHET

Riktlinjer för informationssäkerhet

Bromölla kommun

2013-08-12

INNEHÅLL

1 INLEDNING

Dessa riktlinjer redovisar kommunledningens viljeinriktning och mål för informationssäkerhetsarbetet och syftar till att klarlägga

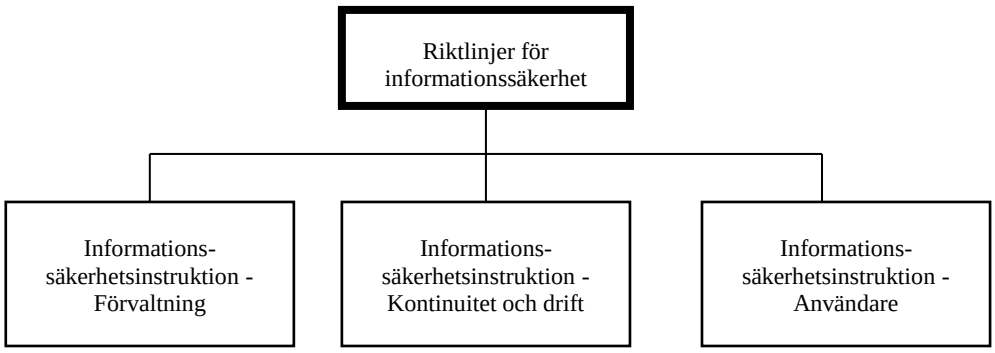
- hur informationssäkerhetsarbetet ska bedrivas,
- mål för informationssäkerhetsarbetet,
- ansvar och roller inom informationssäkerhetsområdet samt
- generella regler och rutiner.

Riktlinjer för informationssäkerhet fastställs av kommunstyrelsen.

Riktlinjerna konkretiseras i

- *Informationssäkerhetsinstruktion - Förvaltning*,
- *Informationssäkerhetsinstruktion - Kontinuitet och drift* samt,
- *Informationssäkerhetsinstruktion - Användare*.

Informationssäkerhetsinstruktionerna fastställs av kommunstyrelsen.



Riktlinjer för informationssäkerhet och informationssäkerhetsinstruktioner

2 ALLMÄNT

Utgångspunkter för informationssäkerhetsarbetet är

- lagar, förordningar och föreskrifter,
- avtal samt
- våra egna krav.

Informationssäkerhetsarbetet ska säkerställa att kommunen kan tillhandahålla relevant information som

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

Informationssäkerhetsarbetet ska inriktas och bedrivas så att det blir en integrerad del av kommunens normala verksamhet. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till säkerhetsarbetet.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgångar.

Dessa riktlinjer är bindande för alla delar av kommunens verksamhet och ger inget utrymme för lokala regler som avviker från dessa.

Den som använder kommunens informationstillgångar på ett sätt som strider mot dessa riktlinjer kan bli föremål för disciplinära åtgärder.

3 MÅL

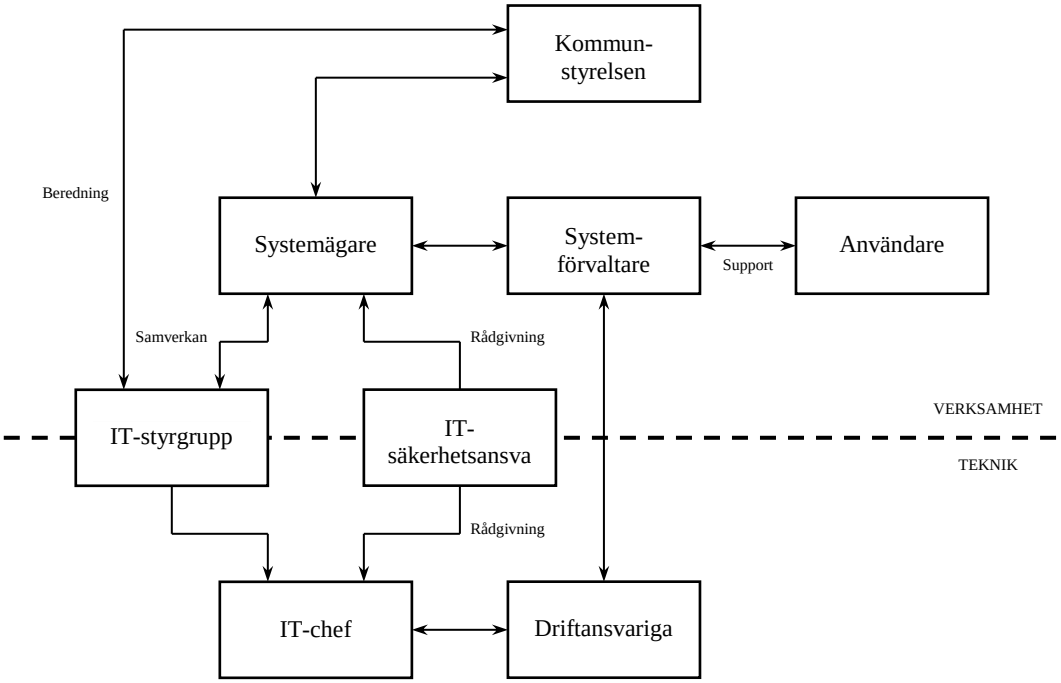
Informationssäkerhetsarbetet ska bedrivas löpande så att

- all personal har kunskap om gällande informationssäkerhetsregler,
- informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man,
- gällande lagar, förordningar och föreskrifter följs,
- ingångna avtal är kända och följs,
- krishanteringsförmågan upprätthålls,
- det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation,
- alla investeringar både i form av information och teknisk utrustning skyddas i tillräcklig grad,
- hotbilden för varje enskilt informationssystem som är av vikt för vår verksamhet analyseras fortlöpande samt att
- händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs

4 ROLLER OCH ANSVAR

Ansvarsfördelningen ska säkerställa att ett IT-system kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stöda avsedd verksamhet och uppfylla målen för informationssäkerhetsarbetet.

Nedanstående bild och efterföljande text beskriver de olika roller och ansvar för informationssäkerheten som finns inom kommunen. Ansvarets omfattning redovisas i *Informationssäkerhetsinstruktion - Förvaltning*.



Roller inom informationssäkerhetsområdet

Det övergripande ansvaret för kommunens IT-system vilar på *kommunstyrelsen*.

På uppdrag av kommunstyrelsen ska *IT-styrgruppen* svara för analys och beredning av IT-frågor.

IT-säkerhetsansvarig utses av kommunstyrelsen.

*Systemägare*n utses av IT-chefen och har ansvaret för att IT-systemet förvaltas på för verksamheten bästa sätt. Systemägaren beslutar om nyanskaffning, vidareutveckling eller avveckling av IT-systemet inom ramen för resurstilldelningen för sin verksamhet.

Vid behov utser systemägaren en *referensgrupp* för sitt IT-system. Referensgruppen fungerar som en rådgivande funktion till systemägaren i frågor som rör systemförvaltningen och håller sig informerad om huruvida systemet stöder verksamheten.

*Systemförvaltare*n utses av systemägaren och har ansvaret för den dagliga användningen av IT-systemet.

Användare av IT-systemet har att följa riktlinjer och instruktioner för informationssäkerheten samt att ta del av och följa de regler som finns för systemet. Se *Informationssäkerhets-instruktion - Användare*.

IT-chefen är systemägare för kommunens tekniska IT-infrastruktur och ansvarar för att denna fungerar.

Driftansvarig utses av IT-chefen och ansvarar för att den dagliga driften upprätthålls enligt överenskommelse med systemägaren. Se *Informationssäkerhetsinstruktion - Kontinuitet och drift*.

För IT-system som är gemensamma för flera kommuner inom Skåne Nordost och/eller Sölvesborgs kommun ska utses *central systemägare*, *central systemförvaltare* och *central driftansvarig*. Dessa ansvarar för samordningen med lokala systemägare, systemförvaltare och driftansvariga i respektive kommun.

5 GENERELLA KRAV

5.1 Utbildning och information

Systemägaren ansvarar för att användarna får nödvändig utbildning i informationssäkerhet.

5.2 Systemförteckning

Samtliga IT-system ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är systemägare, systemförvaltare och driftansvarig.

5.3 Systemanskaffning, -förvaltning och -avveckling

Systemanskaffning, -förvaltning och -avveckling ska följa fastställda rutiner. Se *Informationssäkerhetsinstruktion - Förvaltning*.

5.4 Systemsäkerhetsplan

För samhällsviktiga och/eller Skåne Nordost/Sölvesborgs kommun-gemensamma system ska en systemsäkerhetsplan upprättas. För att bedöma om ett IT-system ska betraktas som samhällsviktigt kartläggs vilken verksamhet som en organisation har krav på sig att bedriva även i fredstida kriser och vid höjd beredskap. Är sådan verksamhet beroende av ett visst IT-system för att kunna upprätthållas på avsedd nivå ska detta IT-system anses vara samhällsviktigt. Systemsäkerhetsplanen fastställs av systemägaren.

5.5 Driftgodkännande

Samhällsviktiga och/eller Skåne Nordost//Sölvesborgs kommun -gemensamma IT-system ska driftgodkännas av systemägaren. Dessförinnan ska systemet granskas för att kontrollera att säkerheten är tillgodosedd i enlighet med kraven i systemsäkerhetsplanen. Beslutet ska dokumenteras.

5.6 Behörighetsadministration

Systemägaren beslutar om behörighet till IT-systemet. Tilldelning, uppföljning, ändring och borttagning av behörighet ska följa fastställd beslutsgång. Se *Informationssäkerhetsinstruktion - Förvaltning*.

5.7 Incidenthantering

Incidenter kan vara interna eller externa intrång och intrångsförsök, felaktig användning av IT-system och IT-resurser med mera. Det är viktigt att kunna återkoppla erfarenheter från incidenter av olika slag för att kunna spåra brister och svagheter.

5.8 Kontinuitetsplanering

Kraven på kontinuitetsplanering framgår av respektive IT-systems systemsäkerhetsplan. Dessa sammanställs i systemsäkerhetsplanen för den tekniska infrastrukturen. Se *Informationssäkerhetsinstruktion - Kontinuitet och drift*.

6. REVIDERING OCH UPPFÖLJNING

Uppföljning är en viktig del i informationssäkerhetsarbetet för att bevaka att

- beslutade åtgärder genomförs,
- regler följs och att
- riktlinjer och instruktioner vid behov revideras.