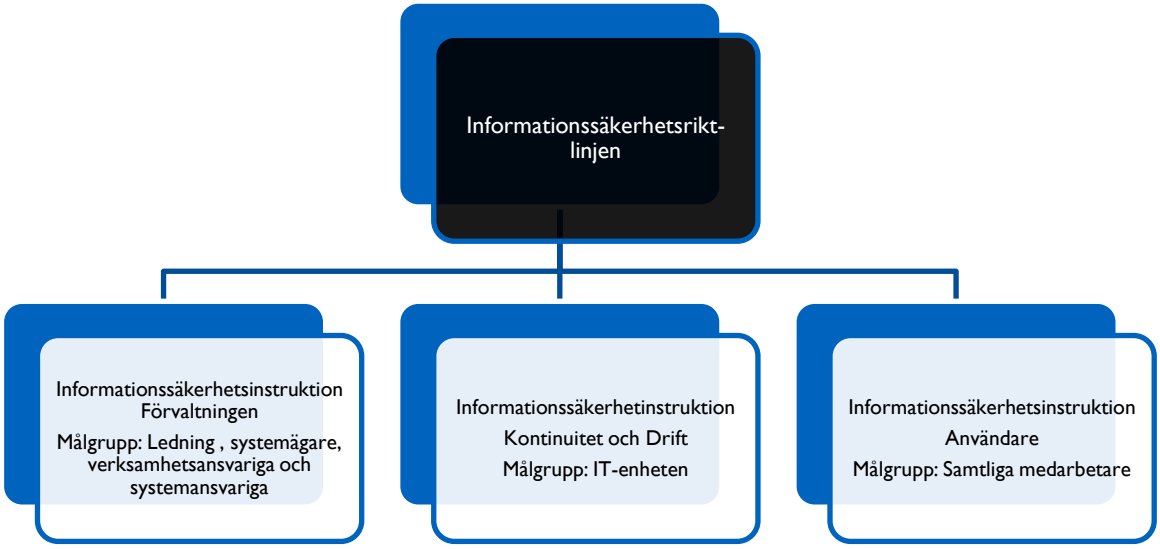
Informationssäkerhet

Dokumenttyp	Riktlinjer
Fastställd/upprättad	2012-02-15 av Kommunstyrelsen § 26
Senast reviderad	2014-02-12 av Kommunstyrelsen § 28
Detta dokument gäller för	Kommunövergripande
Giltighetstid	Tills vidare
Dokumentansvarig	IT-chef
Dnr	2012-68

Innehållsförteckning

Riktlinjens roll i informationssäkerhetsarbetet

Informationssäkerhet är den del i Hjo kommuns lednings- och kvalitetsprocess som avser hantering av verksamhetens information. Informationssäkerhetsriktlinjen och särskilda informationssäkerhetsinstruktioner styr kommunens informationssäkerhetsarbete och ingår i Hjo kommuns verksamhetsskydd.



Informationssäkerhetsriktlinjen redovisar kommunledningens viljeinriktning och mål för informationssäkerhetsarbetet. Riktlinjen konkretiseras i informationssäkerhetsinstruktioner.

Allmänt om informationssäkerhet

Information är en av våra viktigaste tillgångar och hanteringen av den är en viktig del i arbetet med kommunens risk- och sårbarhetsanalys.

Utgångspunkter i vårt arbete med informationssäkerhet är:

- Lagar, förordningar och föreskrifter
- Våra egna krav
- Avtal

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationssäkerheten omfattar kommunens informationstillgångar utan undantag. Med informationssäkerhet avses:

- att rätt information är tillgänglig för rätt person när den behövs och på ett spårbart sätt
- att informationen är och förblir riktig

Informationssäkerheten är en integrerad del av vår 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 kommunens informationstillgångar.

Alla delar inom kommunen är bundna av denna informationssäkerhetsriktlinje vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna.

Den som använder kommunens informationstillgångar på ett sätt som strider mot denna riktlinje kan bli föremål för disciplinära åtgärder

Mål

För kommunens informationssäkerhetsarbete ska gälla att:

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

Roller och ansvar

Kommunchefen har det övergripande ansvaret för informationssäkerheten och utser systemägare för respektive verksamhetssystem.

IT-chefen är direkt underställd kommunchefen samt har det operativa ansvaret för samordning av informationssäkerhetsarbetet.

Systemägaren är den som har ansvaret för den verksamhet som aktuellt verksamhetssystem stödjer.

Systemansvariga utses av respektive systemägare och ansvarar för den dagliga användningen av verksamhetssystemen.

IT-chefen ansvarar för att uppfylla kommunens kontinuitetsplan (Informationssäkerhetsinstruktioner - Kontinuitet och drift) för IT-stödet.

Beskrivning av roller och ansvar framgår av Informationssäkerhetsinstruktion – Förvaltning

Generella krav

Kommunens verksamhetssystem

Samtliga verksamhetssystem ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är systemägare, systemansvarig och avtalstider. IT-enheten ansvarar för att sammanställa informationen om kommunens samtliga verksamhetssystem. Alla verksamhetssystem ska minst klara den basnivå för informationssäkerhet (BITS) som MSB (Myndigheten för Samhällsskydd och Beredskap) rekommenderar.

Informationssäkerhetsutbildning

All personal ska regelbundet få den utbildning som behövs för att informationssäkerheten ska upprätthållas.

Informationsklassning

Information som hanteras på myndigheten ska klassificeras med avseende på sekretess, riktighet och tillgänglighet enligt myndighetens klassningsmodell.

Distansarbete

För att personalen ska kunna arbeta effektivt ska möjlighet finnas att arbeta mobilt eller stationärt på distans. Förutsättningar och restriktioner för detta ska dokumenteras.

Användning av Internet

Endast arbetsrelaterade sidor får besökas. Vid användning av Internet exponeras kommunens namn. Bland annat av detta skäl är det därför av vikt att lägga restriktioner på vilka hemsidor som får besökas. Hemsidor med exempelvis rasistiskt, spel, våldsinriktat eller sexuellt innehåll får inte besökas. Undantag från detta kan beviljas av chef om informationen på sådana sidor kan ha relevans för arbetsuppgifterna.

Elektronisk post

Sekretessbelagd information eller känsliga personuppgifter får inte skickas via okrypterad e-post.

Åtkomst till/av PUL skyddade uppgifter utanför kommunens nät

För åtkomst av PUL skyddade personuppgifter utanför kommunens nät, krävs att användarna identifierar sig med minst två faktorer en s.k. säker inloggning.

Kontinuitetsplanering

Kontinuitetsplaneringen är av central betydelse för att bedriva verksamheten på en acceptabel nivå under såväl normala förhållanden som vid extraordinära händelser. En kontinuitetsplan ska finnas för driften av IT-verksamheten baserad på de olika informationssystemens samlade krav och vara integrerade med kommunens gemensamma kontinuitetsplan.

Revidering och uppföljning

Uppföljning är en viktig del i informationssäkerhetsarbetet för att bevaka att:

- beslutade åtgärder är genomförda
- årliga mål är uppfyllda
- regler följs
- att riktlinjen, säkerhetsinstruktioner och riskanalyser vid behov revideras

Mer information

Mer information finner du i:

- Informationssäkerhetsinstruktion - Förvaltning
- Informationssäkerhetsinstruktion – Kontinuitet och drift
- Informationssäkerhetsinstruktion – Användare
- Säkerhetsreglerna som gäller för specifika verksamhetssystem
- Riktlinjer för sociala medier