

**KARLSTADS KOMMUN****KOMMUNLEDNINGSKONTORET****IT-enheten**

Farid Sajadi

Riktlinjer Informationssäkerhet

Bakgrund

Information är en av koncernen Karlstads kommuns viktigaste tillgångar. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationssäkerheten är en integrerad del av vår verksamhet. Med informationssäkerhet menas den samlade effekten av de skyddsåtgärder, som tillsammans minskar eller eliminerar de hot och risker, som riktar sig mot IT-stödets och informationsresursernas tillgänglighet, riktighet, sekretess och spårbarhet.

Utgångspunkten för arbete med informationssäkerhet är lagar, avtal, förordningar och föreskrifter samt kommunens egna krav. De reglerar hur kommunen, och andra nyttjare av kommunens IT-infrastruktur ska arbeta med informationssäkerhet. De skall vara kända och följas upp kontinuerligt.

Koncernen Karlstads kommun har valt att bygga upp strukturen för informationssäkerhet med stöd av BITS samt utifrån Kris beredskapsmyndighetens rekommendationer.

Syfte

Riktlinjen redovisar ledningens viljeyttring och engagemang gällande informationssäkerhetsarbetet och syftar till att sammanfatta och tydliggöra den säkerhetsnivå som koncernen Karlstads kommun skall ha. I det ingår även roll och ansvarsfördelning.

Mål

Målet är att genom ett strukturerat och väl genomtänkt informationssäkerhetsarbete skydda kommunens information mot oönskade händelser som ger negativa konsekvenser för verksamhet, medborgare och samverkan.

Metod

Karlstads kommun har fattat beslut om att utforma IT säkerhet utifrån Kris beredskapsmyndighetens kvalitetssäkringsmodell, BITS, basnivå.

Denna riktlinje konkretiserar hur informationssäkerhetsinstruktioner skall tas fram och hanteras utifrån KBM/BITS avseende uppdrag, roller/ansvar, granskning och revision.

Roller/ansvar informationssäkerhet

- **Kommunstyrelsen** har det övergripande ansvaret.
- **Nämnd och bolag** har ansvar inom respektive verksamhetsområde.
- **Förvaltningsdirektör VD** organiserar informationssäkerhetsarbetet inom förvaltningen/bolaget samt ansvarar för ledning och kontroll. FD/VD är system- objektsägare och har det övergripande förvaltaransvaret för verksamhetssystem.
- **Objektsägare verksamhet** är ansvariga inom respektive område. De skall själva planera så att resurser avsätts för att policy, riktlinjer och rutiner kan följas
- **Systemförvaltare** har det dagliga ansvaret för systemanvändandet på verksamhetsnivå.
- **IT-chef** är övergripande ansvarig för att beslutade åtgärder gällande infrastruktur och skydd av gemensamma resurser genomförs.
- **IT säkerhetssamordnare** är ansvarig för att samordna informationssäkerhetsarbetet inom koncernen.
- **Användare** ansvarar för att följa kommunens gällande riktlinjer och instruktioner

Uppdrag

Koncernens informationssystem

Samtliga informationssystem ska vara identifierade, förtecknade och bedömda efter vilka som är verksamhetskritiska. Av förteckningen skall en fullständig roll och ansvarsbeskrivning framgå för identifierade system. Alla informationssystem ska minst klara den basnivå för informationssäkerhet som koncernen fattat beslut om.

Informationssäkerhetsutbildning

All personal ska i samband med nyanställning, omplacering och när speciellt behov föreligger få den utbildning som behövs för att informationssäkerheten ska upprätthållas.

Riskbedömningar

Hotbilden för varje enskilt informationssystem som är av vikt för verksamheten skall analyseras fortlöpande, och identifierade händelser som kan leda till negativa konsekvenser skall förebyggas.

Systemsäkerhetsanalyser

Systemsäkerhetsanalyser ska genomföras på identifierade verksamhetskritiska informationssystem.

Incidenthantering

Skade- och incidentrapporteringsrutin skall finnas i koncernen och följas i verksamheten.

Granskning och revision

Kommunens/bolagens revisorer beslutar om åtgärder för att granska informationssäkerhetsarbetet och i samband med revision följa att

- beslutade åtgärder är genomförda
- granskning av kommunikationsresurser, IT system och datorer utförs
- säkerhetsfrågor beaktas vid upprättande av kravspecifikationer och servicenivåavtal (SLA)
- riktlinje och säkerhetsinstruktioner följs
- riktlinje, säkerhetsinstruktioner och riskanalyser vid behov revideras.