MARIESTAD

Informationssäkerhets-policy

Mariestad

Antaget av Kommunfullmäktige
Mariestad 2017-06-12

Inledning

I Mariestads kommuns verksamheter finns stora informationsmängder. Informationen är inte sällan känslig om den sprids till obehöriga, bland annat med hänsyn till enskildas personliga integritet samt att information kan missbrukas för att störa samhällets funktionalitet eller för att tillskansa sig ekonomiska fördelar. Den kommunala verksamheten är därtill ofta beroende av att ha tillgång till rätt information i rätt tid för att på ett effektivt sätt kunna uppfylla sina åtaganden.

Sammantaget finns ett starkt behov av att skydda information från att spridas till fel personer, att skydda information från att förvanskas samt säkerställa att information finns tillgänglig när den behövs i verksamheten. Kommunens informationssäkerhetsarbete ska bidra till det.

Informationssäkerheten ska vara en integrerad del av kommunens verksamheter. Alla som i någon utsträckning hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten.

För att inrikta detta arbete har denna informationssäkerhetspolicy upprättats. Policyn och tillhörande styrdokument omfattar kommunens alla informationstillgångar.

Policyns syfte och mål

Informationssäkerhetspolicyns syfte är att bidra till att den kommunala verksamheten med hjälp av informationstillgångar ska kunna bedrivas på ett effektivt sätt och att dessa tillgångar ska ha ett tillräckligt skydd.

Målet med informationssäkerhetspolicyn är att alla kommunens informationstillgångar ska omfattas av en tillräcklig skyddsnivå med hänsyn till konfidentialitet, riktighet, tillgänglighet och spårbarhet. Rätt information ska finnas tillgänglig när den behövs för behörig person och på ett spårbart sätt.

Ansvar för informationssäkerhet och informationssäkerhetspolicy

Kommunfullmäktige beslutar om informationssäkerhetspolicy för Mariestads kommun. Kommunens nämnder och kommunstyrelsen ansvarar för att informationssäkerheten upprätthålls inom respektive verksamhet. Kommunstyrelsen har uppsiktsplikt över nämnderna.

Nämnderna/bolagsstyrelserna ansvarar för att informationstillgångar inom nämndens/bolagsstyrelsens underliggande verksamheter omgärdas av ett tillräckligt skydd. Respektive nämnd/bolagsstyrelse ska analysera behovet av och eventuellt upprätta regler och rutiner för nämndens/styrelsens verksamheter till stöd för denna policy, utöver vad som ingår i de kommunövergripande styrdokument som antas av kommunens ledningsgrupp.

Sektor- och verksamhetschefer samt bolagschefer kan av nämnd/styrelse delegeras det operativa ansvaret för att driva informationssäkerhetsarbetet.

En chefsbefattning i kommunen innebär ansvar för att underställd personal är informerade om och utbildade i regler kring informationssäkerhet. Det innebär också ansvar för att regler följs inom chefsbefattningens ansvarsområde. I ansvaret ligger också att personer som inte är anställda av men arbetar med och åt kommunen har tillräckligt god kunskap om kommunens regler för informationssäkerhet.

Alla kommunanställda har ansvar för att sätta sig in i och följa aktuella regler för informationssäkerhet.

Den som använder kommunernas informationstillgångar på ett sätt som strider mot denna policy eller övriga styrdokument avseende informationssäkerhet kan bli föremål för åtgärder från kommunernas sida.

Operationalisering av informationssäkerhetspolicyn

Förtydligande styrdokument

Hur informationssäkerhetspolicyns syfte och mål ska nås konkretiseras genom rutiner och regler. Dessa styrdokument antas av kommunchefens ledningsgrupp.

Informationsklassificering

Kommunens informationstillgångar ska klassificeras med hänsyn till krav på konfidentialitet, riktighet, spårbarhet och tillgänglighet. Därigenom kan lämpliga skyddskrav ställas upp för respektive informationstillgång. För de tillgångar som bedöms vara särskilt viktiga ska en informationsägare utses och riskanalyser upprättas. Sektor- och verksamhetschefer samt bolagschefer är ansvarig för att informationsklassning görs.

För de verksamhetssystem som i informationsklassificeringen konstateras vara kritiska för verksamheten ska en systemsäkerhetsplan upprättas och hållas uppdaterad. För informationstillgångar med höga krav på tillgänglighet inkluderar det en avbrottsplan. Sektor- och verksamhetschefer samt bolagschefer är ansvarig för att det görs.

Informationsklassificering ska genomföras innan upphandling av nya verksamhetssystem i syfte att säkerställa relevant kravställning på systemet.

Revision och uppdatering av policyn

Kommunchefen är ansvarig för att behovet av revision av informationssäkerhetspolicyn årligen analyseras samt att vid behov upprätta ett förslag till reviderad policy för beslut i kommunfullmäktige.

Nämnder och styrelse är ansvariga för att efterlevnaden av informationssäkerhets-arbete kontrolleras och att en årlig rapport lämnas till kommunstyrelsen.

Definitioner

Informationstillgångar: en viss informationsmängd/typ av information som är skyddsvärd. Kan vara ett verksamhetssystem om det är starkt knutet till just en typ av information, exempelvis ett journalsystem inom vård- och omsorgsområdet.

Konfidentialitet: information är endast tillgänglig för dem som är behöriga att ta del av och använda den

Riktighet: informationen skyddas mot oönskad och obehörig förändring eller förstörelse.

Spårbarhet: ändringar av information är möjlig att följa i efterhand.

Tillgänglighet: informationen finns tillgänglig enligt verksamhetens krav.