Informationssäkerhetspolicy

Tyresö kommun

2014-xx-xx

tyresö kommun

Innehållsförteckning

Antagen av kommunfullmäktige 2014-xx-xx (§ xx Dnr 2014/KS 0064)

1 Mål för informationssäkerhetsarbetet

Tyresö kommun ska erbjuda en kommunal service som har en hög kvalitet och som är kostnadseffektiv. Tyresö kommun är beroende av att medborgare, företag och övriga intressenter har ett starkt förtroende för verksamheten.

Information är en av kommunens viktigaste tillgångar och hanteringen av den är en viktig del i arbetet. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljö den förekommer i. Det är därför viktigt att information hanteras på ett säkert sätt och inte sprids felaktigt.
En bra informationssäkerhet förbättrar förtroendet för kommunens verksamheter, håller ner direkta och indirekta kostnader samt minskar risken för att säkerhetsrisker och rättsliga processer realiseras.

Policyn vänder sig till kommunens samtliga anställda, förtroendevalda samt annan kontrakterad personal och samarbetspartners som kommer i kontakt med kommunens informationstillgångar.

Policyn beskriver kommunens mål och inriktning för informationssäkerhetsarbetet. Policyn ska konkretiseras med riktlinjer och rutiner som ska ge verksamheten ett stöd kring informationssäkerhet i det dagliga arbetet inom kommunen.

Vårt arbete med informationssäkerhet utgår framförallt från

- lagar, förordningar och föreskrifter
- Tyresö kommuns egna krav
- avtal

2 Policyns syfte

Informationssäkerheten omfattar all verksamhet i Tyresö kommun utan undantag. Syftet med informationssäkerhetsarbetet är att säkerställa följande:

Riktighet: Att upprättad information inte kan förändras vare sig av obehöriga, av misstag eller på grund av funktionsstörning. Informationen ska vara tillförlitlig, korrekt och fullständig.

Sekretess: Att innehållet i dokument, information och handlingar etc. inte görs tillgängliga eller avslöjas för obehörig om den innehåller sekretessuppgifter.

Spårbarhet: Att i efterhand så långt som möjligt kunna härleda specifika aktiviteter eller händelser till identifierade användare, skrivare, dator eller system/program. Det bör gå att se vilka förändringar som har hänt eller gjorts och av vem dessa har utförts.

Tillgänglighet: Att information och informationstillgångar kan utnyttjas efter behov, i förväntad utsträckning och inom önskad tid utifrån de krav som ställs på verksamheten.

Informationssäkerheten är en integrerad del av verksamheten. 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 informationssäkerhetsarbetet.

Den som använder kommunens informationstillgångar på ett sätt som strider mot denna policy kan bli föremål för disciplinära, alternativt rättsliga, åtgärder.

3 Grundprinciper (Mål)

För Tyresö kommuns informationssäkerhetsarbete gäller att:

- personal och förtroendevalda har kunskap om gällande informationssäkerhetspolicy med tillhörande riktlinjer och rutiner.
- berörda elever har kunskap om egna verksamhetens riktlinjer och rutiner.
- informationshanteringen är säker, effektiv och bidrar till ökat skydd och stöd för verksamheten.
- lagar, förordningar, föreskrifter och ingångna avtal ska följas.
- bibehålla informationssäkerheten även vid kris.
- all information samt teknisk utrustning har tillräckligt skydd.
- det finns tillgång till en gemensam, säker och väl definierad infrastruktur (teknisk plattform) för extern och intern datakommunikation.
- hotbilden för varje enskilt informationssystem som är av vikt för verksamheten analyseras fortlöpande.
- händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs.
- informationssäkerhetsarbetet ska ingå i den normala internkontrollen.
- var och en ska vara uppmärksam på och rapportera händelser som kan misstänkas påverka informationssäkerheten.

4 Generella krav

4.1 Kommunens informationstillgångar

Samtliga informationssystem ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är systemägare eller om en informationsägare utsetts. Det framgår i systemförvaltarplanen.

Alla informationssystem ska minst klara de metodstöd för informationssäkerhet som kommunen rekommenderar och som utges av Myndigheten för samhällsskydd och beredskap (MSB).

4.2 Informationssäkerhetsutbildning

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

4.3 Informationsklassning

Information som hanteras i kommunen ska klassificeras med avseende krav på sekretess, riktighet, tillgänglighet och spårbarhet.

4.4 Användning av kommunens informationstillgångar

Samtlig personal och förtroendevalda inom Tyresö kommun som använder kommunens informationstillgångar är skyldiga att känna till och följa kommunens policys, regler och riktlinjer inom informationssäkerhet.

4.5 Riskanalys och kontinuitetsplanering

Med hjälp av riskanalys bedöms sannolikheter för olika oönskade händelser och dess konsekvenser.

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 baserad på de olika informationstillgångarnas samlade krav efter genomförd riskanalys.

För respektive informationstillgång är systemägaren ansvarig för riskanalys och kontinuitetsplanen.

5 Roller och ansvar

Ansvaret för informationssäkerheten ligger i kommunens linjeorganisation, det innebär att:

Kommundirektören har det yttersta ansvaret för informationssäkerheten och att det finns en tydlig ansvarsfördelning för att upprätthålla denna.

Säkerhetschefen har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet.

Informationssäkerhetsansvarig för kommunen är ansvarig för att mallar och riktlinjer utarbetas samt att utbildningsmaterial för informationssäkerhet finns tillgänglig för alla personal och förtroendevalda.

Systemägarna har övergripande ansvar för respektive system och dess användning samt yttersta ansvaret för den information som används av systemen.
Den som är utsedd systemägare kan vara den som har ansvaret för den verksamhet som aktuellt informationssystem stödjer.

Systemansvarig är den som ser till att informationen i systemet klassas i rätt nivå och att systemförvaltaren får kännedom och följer de policy, riktlinjer och rutiner som finns.

Systemförvaltarna har det dagliga ansvaret för informationen i systemet, ser till att policys, riktlinjer och rutiner följs samt upprätthåller säkerhetsnivån som systemet har.

Kommunjuristen och kommunarkivarien är rådgörande för frågor gällande bestämmelserna i tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen samt förvaltningslagen.

Chefer ansvarar för att personal och berörda elever följer policyn med tillhörande riktlinjer och rutiner och ska aktivt verka för en positiv attityd till säkerhetsarbetet.

Redaktörer och administratörer ansvarar för att följa de riktlinjer och rutiner som finns för respektive system.

6 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 personal och förtroendevalda utbildas och informeras.
- informationspolicy, säkerhetsinstruktioner och riskanalyser vid behov revideras.

Uppföljning sker dels genom verksamhetens internrevision och dels genom årlig internkontroll.