Policy för informationssäkerhet

Köpings kommun

Syfte

Denna policy utgör kommunens viljeinriktning för att hantera kommunens information på ett systematiskt och informationssäkert sätt.

.

Dokumenttyp	Policy	**Giltigt till och med**	Tills vidare
Version	1	**Beslutat/antaget datum/§§**	
Dokumentägare		**Beslutat/antaget av**	KF
Dokumentansvarig		**Diarienummer**	KS 2022/724
Gäller för	Köpings kommunkoncern		
Giltig fr.o.m.			

Informationssäkerhetspolicy

Inledning

Information är en av kommunens viktigaste tillgångar och hanteringen av den är en viktig och naturlig del i alla verksamheters dagliga arbete, samt en förutsättning för exempelvis digitalisering och för att verksamheterna ska nå sina mål. Att information som kommunen hanterar i relationer med kommuninvånare, företag och organisationer såväl som inom vår egen organisation är korrekt, utgör en grund för tillit och förtroende. Det är även viktigt att information är tillgänglig när det behövs och att känslig information skyddas för att vi skall kunna fullgöra vårt uppdrag i samhället. Arbetet med informationssäkerhet ska vara långsiktigt och kontinuerligt, omfatta alla delar av kommunens verksamheter och alla de informationstillgångar som vi äger eller hanterar.

Målgrupp

Policyn omfattar förtroendevalda, chefer, medarbetare och uppdragstagare inom Köpings kommun och dess bolag.

Definition av information/informationstillgång

Kommunen är beroende av information för att kunna utföra sitt uppdrag. Information kan exempelvis vara text, ljud, bild, film och tal. Personuppgifter är en vanligt förekommande och skyddsvärd information. Information finns överallt och kan förekomma i många olika former – tryckt eller skrivet på papper, lagrad elektroniskt i IT-utrustning och på lagringsmedia, överföras med post och elektronisk utrustning, yttras i en konversation och vara en del av en persons kunskap.

Definition av informationssäkerhet

Informationssäkerhet handlar om att skydda kommunens information så att:

- informationen alltid finns när vi behöver den (tillgänglighet)
- informationen är korrekt och inte manipulerad eller förstörd (riktighet)
- endast behöriga personer kan ta del av informationen (konfidentialitet)

Ansvar

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret.

Kommunfullmäktige uttrycker sin viljeinriktning rörande kommunens arbete med informationssäkerhet i denna policy.

Kommunstyrelsen ansvarar för att samordna och följa upp kommunens informationssäkerhetsarbete. Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta och följa upp policy för informationssäkerhet.

Nämnderna/styrelserna Varje enskild nämnd ansvarar för den information och de informationssystem som finns inom det egna verksamhetsområdet.

Medarbetare, förtroendevalda, elever och uppdragstagare ansvarar för att följa de informationssäkerhetsanvisningar och instruktioner som finns samt att agera säkerhetsmedvetet.

Strategiska mål med informationssäkerhet

Köpings kommun ska bedriva ett långsiktigt och systematiskt informationssäkerhetsarbete, vilket bygger på etablerade standarden för informationssäkerhet (ISO 27000-serien).

Målsättning

- Kommunens information skyddas på en lämplig administrativ och teknisk nivå, utifrån genomförda informationssäkerhetsklassificeringar och riskanalyser
- Det finns en organisation med tydlig fördelning av ansvar för informationstillgångar och med relevanta roller för ledning och genomförande av ett systematiskt informationssäkerhetsarbete.
- Medarbetare, förtroendevalda, elever och uppdragstagare ska genomgå relevant utbildning inom informationssäkerhet

Principer för informationssäkerhet

Informationssäkerhetsarbetet i kommunen ska bedrivas systematiskt, formaliserat och riskorienterat. Informationssäkerhet är en grundförutsättning för att uppnå kvalitet och effektivitet i verksamheten, samt en förutsättning vid upphandling, digitalisering och mobilitet. Informationssäkerhetsarbetet ska skydda kommunens information.

Uppföljning

Kommunen ska följa upp informationssäkerhetsarbetet genom att rapportera avvikelser, åtgärda informationssäkerhetsbrister och i förekommande fall rapportera incidenter till berörda myndigheter.

Efterlevnad

Informationssäkerhetssamordnare ska två gånger per år rapportera läge och status gällande informationssäkerhet till Kommunstyrelsen och till Kommundirektörens ledningsgrupp. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar. Efterlevnaden av informationssäkerhetsarbetet ska också följas upp via internkontroll.

Roller

Nedan beskrivs informationssäkerhetsansvaret för ett antal roller.

Kommunchef har det övergripande ansvaret för informationssäkerheten och att det finns en tydlig ansvarsfördelning för att upprätthålla säkerheten.

Informationsägare är den som bestämmer ändamålen för behandlingen och hanteringen av informationen. Informationsägaren äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids.

Systemägare har ansvaret för den verksamhet som aktuellt informationssystem/-objekt stödjer.

Förvaltningsledare/Systemförvaltare tar det funktionella (dagliga) helhetsansvaret för ett system/objekt. Förvaltaren fungerar i hög grad som system-/objektägarens utförare och ser till att systemets/objektets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.

Säkerhetsskyddschef ansvarar för informationssäkerheten i verksamhet som har betydelse för Sveriges säkerhet och lyder under säkerhetsskyddslagen.

Krisberedskapssamordnare genomför säkerhetsanalyser på uppdrag av säkerhetsskyddschefen.

Dataskyddsombudets roll är att säkerställa att dataskyddsförordningen följs inom kommen genom att utföra kontroller och informationsinsatser.

Informationssäkerhetsamordnare har det övergripande ansvaret för att leda, utveckla och samordna arbetet med informationssäkerhet i kommunen. Stödfunktion för ledning och verksamheter.

IT-chef har det operativa ansvaret för att uppfylla de krav som verksamheten ställer på den tekniska IT-infrastrukturen. IT-chefen eller motsvarande har ett särskilt ansvar för den tekniska IT-säkerheten.

Dataskyddshandläggare, inom varje nämnd ska det finnas ett utsett dataskyddshandläggare vilket har ansvaret att dokumentera sin nämnds behandlingar av personuppgifter i en registerförteckning.