Informationssäkerhet och dataskydd

POLICY

FALKÖPING KOMMUNEN

Typ av styrdokument	Policy
Beslutsinstans	Kommunfullmäktige
Fastställd	2023-09-25, § 67
Diarienummer	KS 2023/654
Giltighetstid	Fr.o.m 2023-10-15 och tillsvidare
Dokumentet gäller för	Samtliga nämnder och förvaltningar i kommunen
Dokumentansvarig	Kanslichef
Tidpunkt för aktualitetsprövning	Vid behov

Innehåll

Inledning

Information är en av kommunens viktigaste tillgångar och en förutsättning för att kommunens verksamheter ska kunna bedrivas, effektiviseras och nå sina mål. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer. Exempel på information kan vara i form av text, ljud, bilder eller film, och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal. Av all information som kommunen hanterar utgör en stor del behandling av personuppgifter vilket ställer krav på kommunens dataskyddsarbete.

Informationssäkerhetsarbetet ska vara ett effektivt stöd i verksamheten. För att nå hög kvalitet i arbetet måste informationen hanteras på rätt sätt. Lagar och förordningar utgör grunden för detta arbete samt överenskomna avtal.

Syftet med informationssäkerhetsarbetet är att skydda kommunens verksamheter mot skador och avbrott medan dataskyddsarbetets syftar till att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Genom ett förebyggande arbete med informationssäkerhet ges verksamheterna bättre möjligheter att hantera gällande lagkrav och bevara förtroendet för kommunen samtidigt minimeras negativa och oönskade händelser.

Ett väl fungerande informationssäkerhetsarbete är en förutsättning för dataskyddsarbetet. Genom att samordna informationssäkerhetsarbetet och dataskyddsarbetet skapas därför goda förutsättningar att uppfylla de krav som ställs. Ett systematiskt informationssäkerhets- och dataskyddsarbete skapar också förutsättningar för verksamhetsutveckling inom flera områden.

Arbetet med informationssäkerhet innebär att vidta fysiska, tekniska, administrativa och organisatoriska åtgärder för att uppnå eller bevara rätt skydd av informationstillgången. Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån följande aspekter:

Tillgänglighet innebär att information är åtkomlig och användbar för behörig person vid rätt tillfälle.

Konfidentialitet innebär att informationen inte tillgängliggörs eller avslöjas för obehörig person.

Riktighet innebär att informationen är korrekt och fullständig för behörig person och skyddas mot oönskad förändring.

Om policyn

Denna policy redovisar Falköpings kommuns viljeinriktning och övergripande mål med informationssäkerhetsarbetet och dataskyddsarbetet.

Policyn omfattar all information som kommunens verksamhet äger och hanterar, utan undantag.

Alla medarbetare och förtroendevalda ska agera i enlighet med denna policy när de hanterar kommunens informationstillgångar.

Policyn och underliggande styrdokument för informationssäkerhet och dataskydd samt övriga styrande dokument vilka angränsar till informationssäkerhetsarbetet ger de kommunala verksamheterna stöd i det dagliga arbetet.

Strategisk inriktning

Falköpings kommun strategiska mål med informationssäkerhet och dataskydd är följande:

- Det ska bedrivas ett systematiskt informationssäkerhetsarbete och dataskyddsarbete.

- Det ska arbetas förebyggande mot oönskade händelser.

- Det ska finnas en organisation för informationssäkerhet och dataskydd med relevanta roller som är kända och aktiva i verksamheten.

- Det ska finnas en grundläggande kompetens kring informationssäkerhet och dataskydd hos alla medarbetare i kommunen.

Systematiskt informationssäkerhetsarbete och dataskyddsarbete

För att Falköpings kommun ska uppfylla och säkerställa den strategiska inriktningen i policyn ska arbetet med informationssäkerhet och dataskydd genomföras enligt följande:

- Kommunens informationssäkerhetsarbetes ska uppfylla de grundläggande kraven i standarden ISO 27000 enligt rekommendation från Myndigheten för samhällsskydd och beredskap (MSB).

- Kommunen ska arbeta proaktivt samt ha en god förmåga att kunna hantera och rapportera incidenter, allvarliga störningar och kriser.

- Genom omvärldsbevakning ska kommunen hålla sig uppdaterad med aktuell lagstiftning, förordningar och föreskrifter samt aktivt delta i nätverk och implementera kunskapen i informationssäkerhetsarbetet och dataskyddsarbetet.

- Kommunen ska upprätta de styrdokument som behövs för ett systematiskt informationssäkerhets- och dataskyddsarbete.

- Kommunen ska ställa informationssäkerhets- och dataskyddskrav inför upphandling, utveckling, användning och avveckling av system för informationstillgångar. Kraven ska kontinuerligt följas upp.

- Alla medarbetare och förtroendevalda ska erbjudas relevant utbildning inom informationssäkerhet och dataskydd. Information och utbildning bidrar till att upprätthålla en hög säkerhetskultur inom kommunen och ger förutsättningar för berörda att leva upp till denna policy och övriga styrdokument.

Ansvar och roller

Respektive nämnd i kommunen är ytterst ansvarig för att dess verksamhet håller rätt och relevant nivå på informationssäkerheten och dataskyddet. Nämnderna är personuppgiftsansvariga vilket innebär att de har det yttersta ansvaret för att personuppgiftsbehandlingen inom respektive nämnds verksamhetsområde. Nämnderna ansvarar också för att tillräckliga resurser finns allokerade.

För genomförandet av rätt och relevant informationssäkerhets- och dataskyddsarbete ansvarar chefer i enlighet med delegationsordningen.

Kommunfullmäktige har det övergripande ansvaret för kommunens informationssäkerhet. Det innebär att kommunfullmäktige fastställer en strategisk inriktning genom denna policy.

Kommunstyrelsen ansvarar för att informationssäkerhetsarbetet och dataskyddsarbetet leds och samordnas. Kommunstyrelsen har ansvar för uppföljning och beslutar om riktlinjer.

Informationsägare är den som äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids. Informationsägaren är därmed riskägare för den information som ska hanteras i IT-systemet/lösningen. För att hantera risken bör informationsägaren genomföra en riskanalys.

Medarbetare och förtroendevalda har ett ansvar att följa kommunens policy och underliggande styrdokument för informationssäkerhet och dataskydd. Medarbetare och förtroendevald har också ansvar för att vara uppmärksam på brister och fel gällande informationshantering, utrustning samt informationsinnehåll och rapportera sådana i enlighet med fastställda rutiner.