Informationssäkerhetspolicy

Dokumenttyp	Policy
Fastställd/upprättad	Kommunfullmäktige 2023-06-29, § 140
Senast reviderad	
Detta dokument gäller för	Kommunövergripande
Giltighetstid	Tills vidare
Dokumentansvarig	IT-chef
Dnr	2023-177

Innehållsförteckning

Informationssäkerhetspolicy

Denna policy är ett övergripande dokument som anger Hjo kommuns viljeinriktning och mål för informationssäkerhetsarbetet. Policyn gäller samtliga informationstillgångar som hanteras av kommunens verksamheter oavsett om den är muntlig, pappersbunden eller digital.
Policyn och dess tillhörande styrdokument omfattar därutöver samtliga personer som är i kontakt med kommunens informationstillgångar. Policyn och dess kompletterande förtydligande rutiner ger kommunens verksamheter stöd i informationssäkerhetsarbetet samt förutsättningar att nå uppsatta mål. Ansvaret för informationssäkerhetsarbetet i kommunen följer verksamheten dvs linjeansvaret, vilket innebär att respektive verksamhetschef/stabschef ska analysera behovet av och ta fram rutiner/instruktioner för informationssäkerhetsarbetet, exempelvis rutiner/instruktioner för behörighetstilldelning i verksamhetssystem.
Policyn följer nationellt antagna lagar och regler exempelvis Dataskyddsförordningen, Arkivlagen, Tryckfrihetsförordningen, Sekretesslagen, Säkerhetsskyddslagen.

Om informationssäkerhet

Informationen som kommunens verksamheter hanterar ska vara tillgänglig, riktig, spårbar samt konfidentiell. Det innebär att rätt information ska vara tillgänglig för rätt person vid rätt tidpunkt.
En avvikelse mot någon av dessa påverkar informationssäkerheten. En påverkan som kan leda till konsekvenser för exempelvis personlig integritet, förtroende för kommunen, driftsstörningar i samhällsviktig verksamhet.
Informationssäkerhet är en förutsättning för att kommunens verksamheter ska kunna leverera vård och omsorg, utbildning eller annan kommunal service.

Mål för informationssäkerhetsarbetet

Målet med Hjo kommuns informationssäkerhetsarbete är att informationen som hanteras inom verksamheterna följer grundprinciperna om tillgänglighet, riktighet, spårbarhet och konfidentialitet.

Konkretiserat innebär det att Hjo kommun ska nå och upprätthålla en nivå inom informationssäkerhetsarbetet som:

- efterlever nationellt antagna lagar, förordningar, föreskrifter samt avtal,
- efterlever internationella standarderna SS-ISO/IEC 27001 och 27002,
- skyddar informationstillgångar i nivå med dess värde samt i relation till eventuella konsekvenser,
- tar höjd för en systematisk och kontinuerlig efterlevnad, vilket innebär återkommande årliga revideringar av rutin/instruktioner, klassningar etc.

Strategier för att nå målet

Hjo kommun ska nå informationssäkerhetsmålet genom att använda sig av följande strategier:

- Klassificering av samtliga informationstillgångar, avgör och prioriterar adekvata och korrekta säkerhetsåtgärder,
- Kontinuitetsplaner för samtliga informationsflöden, -tillgångar och -mängder,
- Incidentrapportering, -uppföljning, -åtgärder,
- Förankring/ information och utbildning genomförs systematiskt och kontinuerligt i hela organisationen.

Roller och ansvar

Informationssäkerhet är en integrerad del av det dagliga arbetet som bedrivs inom Hjo kommuns organisation. Alla som på något sätt kommer i kontakt med information har en skyldighet och ett ansvar att hantera denna information på ett säkert sätt.
Hjo kommuns IT-chef tillika informationssäkerhetsansvarig samt övrig personal som arbetar med relaterade områden såsom IT-säkerhet, dataskydd, sekretess etc. fungerar som ett stöd till kommunens verksamheter i deras arbete med att fullfölja informationssäkerhetsansvaret.
Kommunfullmäktige beslutar om informationssäkerhetspolicyn för Hjo kommun. Det är varje verksamhets ansvar att informationssäkerheten efterlevs i enlighet med fastslagna policy och rutiner.

Följande roller är centrala för det strategiska och operativa informationssäkerhetsarbetet i Hjo kommun:

- **Kommunfullmäktige** fastställer kommunens policy för informationssäkerhet.
- **Kommunstyrelsen** ansvarar för:
    - övergripande arbetet med informationssäkerhet,
    - efterlevnad och uppföljning och policy,
    - personuppgiftsansvarig och därmed formellt föremål för eventuell tillsyn.
- **Verksamhetschef/-ledningsgrupp** bedömer och beslutar om behovet av verksamhetsspecifika rutiner/ instruktioner.
- **Chefer** ansvarar för att informationssäkerhetsarbetet bedrivs i linje med denna policy, övergripande rutin och lokalt förekommande rutiner/instruktioner.
- **IT-chef** övergripande ansvar för att tillmötesgå de krav som policy och rutin ställer på den tekniska IT-infrastrukturen.
- **System-** och **informationsägare** har det övergripande ansvaret för respektive system samt dess information. Systemen och informationshanteringen ska uppfylla informationssäkerhetskraven. System- och informationsägarskapet följer verksamhetsansvaret.
- **Systemansvarig** utses av systemägare.
- **Dataskyddsombudsfunktionen** övervakar verksamheternas efterlevnad av dataskyddslagstiftningen samt ger råd och vägledning.
- **Informationssäkerhetssamordnare/**dataskyddssamordnare ansvarar för övergripande samordning av informationssäkerhetsarbetet och övervakar att informationssäkerhetspolicy samt tillhörande rutinen följs.
- **Kontaktpersoner** för informationssäkerhet och dataskydd. Verksamheterna tillser att en ändamålsenlig organisation finns för informationssäkerhet och dataskydd genom att utse kontaktpersoner som ansvarar för det löpande operativa arbetet.
- **Medarbetare och förtroendevalda** är skyldiga att följa policy, rutiner och instruktioner för informationssäkerhet och dataskydd.

Den som använder kommunens informationstillgångar eller i övrigt agerar på ett sätts om strider mot denna policy eller övriga styrdokument avseende informationssäkerhet kan bli föremål för arbetsrättsliga påföljder. Vid misstanke om brott görs polisanmälan.

Uppföljning och rapportering

Informationssäkerhetspolicyn och tillhörande rutin ska granskas och revideras minst vart tredje år, eller vid de tillfälle då betydande förändringar i organisationen eller omvärlden sker. Detta för att säkerställa policyns och rutinens fortsatta lämplighet, riktighet och verkan.

Informationssäkerhetsamordnaren ska årligen rapportera läge och status gällande informationssäkerheten till kommunstyrelsen. Särskilda skäl, såsom exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapportering.