Administrativa enheten
Emmy Johansson
emmy.johansson@svalov.se

POLICY

Datum
2024-09-30

Diarienummer
231-2021:340

Antagen av kommunfullmäktige
2024-11-25 § 256

Informationssäkerhetspolicy

Dokumentinformation

Diarienummer: KS 231-2021

För revidering ansvarar: Kommunfullmäktige

För uppföljning ansvarar: Kommunfullmäktige

Dokumentansvarig: Enhetschef kansli

Dokumentet gäller för: Alla kommunens verksamheter

Giltighetsperiod: 2024-11-25 - tillsvidare

Aktualitetsprövas/revideras: En gång per mandatperiod samt vid behov

Ersätter: Informationssäkerhetspolicy daterad 2015-08-17

Publicerat i kommunal författningssamling: 2024-12-06

Antaget: KF 2024-11-25 § 256

Inledning

Informationstillgångar är en grundläggande förutsättning för att kommunal verksamhet ska kunna bedrivas effektivt enligt gällande lagar och förordningar. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationssäkerheten är en del i kommunens lednings- och kvalitetsarbete och omfattar alla informationstillgångar utan undantag. Informationssäkerhet är förmågan att upprätthålla önskad sekretess, riktighet och tillgänglighet avseende informationstillgångar.

Informationssäkerhet utgörs bland annat av teknisk säkerhet, men även av administrativ säkerhet. Teknisk säkerhet utgörs av IT-säkerhet och av fysisk säkerhet i till exempel lokaler. Administrativ säkerhet innebär formell säkerhet i form av riktlinjer och rutiner men även informell säkerhet så som en god säkerhetskultur där verksamheten är medveten om vikten av att arbeta informationssäkert.

Utgångspunkt

Svalövs kommuns informationssäkerhetsarbete ska i linje med rekommendationer från Myndigheten för samhällsskydd och beredskap (MSB) samt den etablerade standarden SS-ISO/IEC 27000 utgå från följande ledord:

- **Tillgänglighet**. Information ska finnas tillgänglig när den behövs och på förväntat sätt.
- **Riktighet**. Vår information ska vara korrekt och tillförlitlig. Informationen ska skyddas mot oönskad förändring och förstöring.
- **Spårbarhet**. Aktiviteter ska kunna härledas i efterhand. Vi ska kunna visa vad som har hänt och vem som har gjort vad i våra system.
- **Konfidentialitet**. Vår information ska inte göras tillgänglig eller avslöjas för obehöriga.

Utöver dessa ledord ska informationssäkerhetsarbetet även bedrivas utifrån gällande lagstiftning så som dataskyddsförordningen (GDPR)[1], NIS-direktiv[2] samt sektorsspecifika lagar och förordningar för respektive nämnd. Inom ramen för gällande lagstiftning ställs det krav på att informationssäkerhetsarbetet ska bedrivas systematiskt genom bland annat incidentrapportering och -hantering, riskanalyser och olika säkerhetsåtgärder för att säkerställa att vår information hanteras och skyddas på ett säkert sätt.

Mål

Det övergripande målet med denna policy är att beskriva kommunens arbete och organisation för informationssäkerhet.

Målet med kommunens informationssäkerhetsarbete är att respektive verksamhets information hanteras korrekt i det dagliga arbetet och vid störningar av olika slag. Informationshanteringen måste vara tillräckligt säker, effektiv och skyddad utifrån den typ av information som avses. Arbetet med informationssäkerhet ska bedrivas strukturerat och systematiskt utifrån gällande policy, riktlinjer och rutiner samt följas upp årligen.

---

[1] EU:s allmänna dataskyddsförordning (EU/2016/679)
[2] Direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela EU.

För informationssäkerhetsarbetet ska gälla att:

- personalen har kunskap om gällande regler för informationssäkerhet
- informationshanteringen är säker, effektiv och bidrar till skydd och stöd för medarbetare, samverkande partners och tredje man
- det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation
- information, system och teknisk utrustning har skydd i tillräcklig grad både digitalt och fysiskt
- hotbilden för information, system och teknisk utrustning analyseras fortlöpande
- händelser i systemen som kan leda till negativa konsekvenser förebyggs

Dokumentstruktur

Informationssäkerhetspolicyn är ett kommunövergripande styrdokument och utgör grunden för arbetet med att skydda och säkerställa kommunens informationstillgångar. Policyn gäller samtliga anställda inom kommunen. Policyn kompletteras med en kommunövergripande riktlinje som ska fungerar vägledande för samtliga nämnder. Den kommunövergripande riktlinjen kan konkretiseras ytterligare i sektorsspecifika riktlinjer och/eller rutiner vid behov. Policyn revideras av informationssäkerhetssamordnare en gång per mandatperiod eller vid större organisatoriska förändringar.

Arkivreglemente och nämndernas informationshanteringsplaner styr informationshanteringen och utgör därmed de grundläggande förutsättningarna för informationssäkerhet.

Andra styrdokument som kompletterar informationssäkerhetspolicyn och underliggande riktlinjer och rutiner är:

- Dataskyddspolicy med tillhörande rutiner för hantering av personuppgifter, incidenter och dataskyddsorganisering
- Digitaliseringsstrategi
- IT-strategi
- Säkerhetspolicy

Inget av styrdokumenten får utformas på så vis att de lämnar konkurrerande eller vilseledande information om hantering av information.

Organisation, roller och ansvarsfördelning

Genom att tydliggöra hur organisationen kring informationssäkerhet är uppbyggd i form av roller och ansvar ökar möjligheten för att kunna säkerställa att kommunens informationstillgångar administreras och hanteras på ett riktigt, säkert och ändamålsenligt sätt.

Kommunfullmäktige fastställer informationssäkerhetspolicyn

Kommunstyrelsen har det övergripande ansvaret för informationssäkerhetsarbetet i kommunen.

Respektive nämnd har det yttersta ansvaret för att bedriva ett systematiskt informationssäkerhetsarbete och ansvarar för den egna verksamhetsinformationen. Informationssäkerhetsansvaret ska följa

verksamhetsansvaret i form av delegationsordning. Ansvarig för en viss nämnd, avdelning och så vidare ansvarar också för informationssäkerheten inom sitt område.

Övergripande principer för informationssäkerhetsarbetet

Varje nämnd ansvarar för att självständigt bedriva ett systematiskt informationssäkerhetsarbete. Informationssäkerhet ska tas i beaktan vid all informationshantering. Nedan följer några kommunövergripande och grundläggande principer för arbetet med informationssäkerhet.

Utbildning

All personal ska genomgå grundläggande utbildning i informationssäkerhet.

Informationsklassning

Informationsklassning innebär att verksamheten klassar sina informationstillgångar utifrån interna och externa krav på konfidentialitet, riktighet och tillgänglighet. Genom att klassa information kan verksamheten identifiera känslig och kritisk information och säkerställa att denna får tillräckligt skydd, men ibland också för att undvika att information får onödigt överskydd. För att veta hur skyddsvärd en informationstillgång är ska den klassas utifrån en förutbestämd mall som gäller för hela kommunen.

Konsekvensbedömning

För att bedöma informationssäkerhetsrisker innan införande av ett nytt system eller arbetssätt ska en konsekvensbedömning, en DPIA göras. DPIA står för Data Protection Impact Assessment och görs för att bedöma risker kring personuppgiftsbehandling men analysen innefattar även informationssäkerhet. En DPIA handlar om att vara förutseende och att förebygga risker för att skydda människors fri- och rättigheter gällande personuppgiftsbehandling och i förlängningen informationssäkerhet.

Informationshanteringsplan

Varje nämnd ska ha en informationshanteringsplan som beskriver hantering, arkivering och gallring av allmänna handlingar.

Kontinuitetshantering

För de system som genom exempelvis risk- och sårbarhetsanalyser identifieras som kritiska för att upprätthålla en tolerabel nivå i verksamheten ska det finnas en plan för hantering av verksamhetens kontinuitet vid incident eller driftsbortfall.

Informationssäkerhetsincidenter

All form av incidenter som kan inträffa i verksamheten så som personuppgiftsincidenter, avvikelser för enskild eller IT-incidenter kan innebära en informationssäkerhetsincident. Hantering av incidenter ska ske enligt de etablerade rutiner för rapportering som finns i verksamheterna.

Upphandling

Vid upphandling ska tillräckliga krav ställas på informationssäkerhet i form av hur väl organisationens information skyddas av leverantören.

Säkerhet

Personal

Kommunen ska försäkras sig om att personal som arbetar inom kommunens verksamheter har en adekvat erfarenhetsnivå och kompetens för dess uppdrag. Personal inom kommunens verksamheter ska enbart ha tillgång till den information som krävs för uppdraget.

Fysisk säkerhet

Kommunens lokaler ska ha erforderliga skyddsåtgärder för att hindra obehörigt tillträde. Tillträde till utrymmen där det finns informationstillgångar av känslig karaktär ska begränsas.

Programvara, utrustning, dokument eller annan lagringsmedia som innehåller känslig information ska hanteras på ett säkert sätt och som utgångspunkt inte avlägsnas från kommunens lokaler. Likaså ska dokument och handlingar med känslig information skrivas ut genom privat utskrift för att skyddas från obehöriga.

IT-säkerhet

Systemdrift och serverutrymme ska lokaliseras i utrymme som är försedda med tillträdes- och brandskydd, fukt och temperaturreglering samt elförsörjning utan avbrott. Det ska även finnas regler för säkerhetskopiering samt kontinuitetsplanering vid behov för servrar och system.

För att säkerställa att system bibehåller en god nivå ska en systemägare och en systemförvaltare utses för respektive system.

Uppföljning

För att informationssäkerhetsarbetet ska bedrivas systematiskt är det viktigt att det följs upp regelbundet. Varje nämnd ansvarar för att arbetet med informationssäkerhet följs upp inom de egna verksamheterna årligen och vid behov.

Kommunstyrelsen ska en gång per tertial få en rapport om hur arbetet med informationssäkerhet fortlöpt under året.