Essunga kommun

Informationssäkerhet-Policy

Dokumenttyp **Fastställd**	Policy Av Kommunfullmäktige 2019-10-21, § 112
Detta dokument gäller för	Essunga kommun
Giltighetstid	Gäller tillsvidare, revidering vart fjärde år. Se ”Riktlinjer för styrdokument”
Dokumentansvarig	
Dnr	2019 - 000234

Innehållsförteckning

1. Inledning

Information är en av kommunens viktigaste tillgångar och en väsentlig förutsättning för att kunna bedriva verksamheten. Kommunens informationstillgångar måste därför behandlas och skyddas på ett tillfredsställande sätt.

Informationen ska bevaras utifrån tre informationssäkerhetsaspekter:

Konfidentialitet: att information enbart är tillgänglig för behöriga.
Riktighet: att information är korrekt, aktuell och fullständig.
Tillgänglighet: att information är åtkomlig i rätt tid och användbar av behörig.

2. Lagstiftning

På övergripande nivå finns krav på informationssäkerhet i Dataskyddsförordningen (GDPR) och Lag om informationssäkerhet i samhällsviktiga och digitala tjänster (NIS-direktivet.) samt Säkerhetsskyddslagen. Därutöver finns verksamhetsspecifika krav på informationssäkerhet i bland annat i skollagen, socialtjänstlagen och hälso- och sjukvårdslagen.

Dataskyddsförordningen ställer krav på hantering av personuppgifter. Informationstillgångar som lyder under NIS-direktivet är de som berör leverantörer av samhällsviktiga tjänster. Till kommunens samhällsviktiga tjänster räknas energi, hälso- och sjukvård samt leverans och distribution av dricksvatten om de uppfyller vissa kriterier.

Säkerhetsskyddslagen avser Sveriges säkerhet och berör bara säkerhetskänsliga verksamheter. Skollagen, socialtjänstlagen och hälso-och sjukvårdslagen ställer krav på tystnadsplikt och sekretess.

3. Intressenter

Informationssäkerhetsarbetet stöds och följs upp från flera myndigheter och organisationer.

- Myndigheten för samhällsskydd och beredskap (MSB)
- Sveriges kommuner och landsting (SKL)
- Datainspektionen (DI)

NIS-direktivet följs även upp av Statens energimyndighet, Livsmedelsverket och Inspektionen för vård och omsorg (IVO). Säkerhetsskyddslagen följs upp av Säkerhetspolisen.

4. Policy

Denna policy utgör kommunens viljeinriktning för att hantera kommunens information på ett systematiskt och informationssäkert sätt. Kommunens informationssäkerhetpolicy omfattar all information kommunens verksamheter äger och hanterar. Information är en av kommunens viktigaste tillgångar och är en förutsättning för att kommunens verksamheter ska kunna bedrivas, effektiviseras och nå sina mål. Informationssäkerhetsarbetet ska vara ett effektivt stöd i kärnverksamheten.

Det systematiska arbetet med informationssäkerhet ska utgå från standarden för informationssäkerhet enligt ISO 27000-serien och integreras i kommunens ledningssystem.

Lagar och förordningar utgör en grund för detta arbete, överenskomna avtal ska följas och medborgarnas krav och förväntningar införlivas.
Informationssäkerhetsarbetet ska bedrivas så det stödjer kommunernas arbete med digitalisering samtidigt som det skyddar kommunens, medarbetarnas och kunderna/brukarnas information.

Ansvaret för informationssäkerheten ska följa verksamhetsansvaret. Alla chefer, medarbetare och förtroendevalda ansvarar för att denna policy och tillhörande riktlinjer följs då de hanterar kommunens informationstillgångar.

Informationssäkerhetsarbetet ska säkerställa att informationstillgångarna skyddas utifrån informationstillgångens skyddsvärde oavsett om den hanteras manuellt eller digitalt.

För att säkerställa de grundläggande kraven och rekommendationerna i denna policy uppfylls har följande strategiska målsättningar formulerats:

4.1 Strategiska målsättningar

Systematiskt informationssäkerhetsarbete

Kommunens ledningssystem för informationssäkerhet ska uppfylla de grundläggande kraven på systematiskt informationssäkerhetsarbete enligt ISO 27000-serien och kommunen ska tillämpa ett arbetssätt som stödjer ständiga förbättringar.

Kommunen ska uppfylla nuvarande och tillkommande lagkrav som berör kommunen och som kräver ett systematiskt informationssäkerhetsarbete.

Organisation

Kommunen ska upprätta en organisation med tydlig fördelning av ansvar för informationstillgångar och med relevanta roller för ledning och genomförande av ett systematiskt informationssäkerhetsarbete. Ansvaret för informationssäkerheten ska utgå från verksamhetsansvaret och hanteras i kommunens delegationsordning. En riktlinje ska finnas som beskriver organisation och roller för informationssäkerhetsarbetet.

Chefer, medarbetare och förtroendevalda

Samtliga chefer, medarbetare och förtroendevalda ska erbjudas relevant utbildning inom informationssäkerhet. Utbildningarna ska samordnas via informationssäkerhetssamordnaren. Chefer ansvarar för att medarbetare har rätt behörighet och förutsättningar att i sitt arbete hantera kommunens informationstillgångar.

Kommunen ska fastställa informationssäkerhetsrelaterade krav på bakgrundskontroll för befattningar. Bakgrundskontroller ska vara anpassade till olika befattningar beroende på vilken information medarbetaren ges tillgång till.

Kommunen ska sträva efter att skapa en god säkerhetskultur i hela organisationen. Detta uppnås främst genom styrande dokument, personal utbildad inom informationssäkerhet samt hantering av avvikelser och risker som underlag till ständiga förbättringar.

Det ska finnas ett fungerande samspel mellan olika kompetenser inom säkerhet, informationssäkerhet, IT, juridik och ledning. Riktlinjer ska finnas för informationssäkerhet för medarbetare och förtroendevalda.

Hantering av informationstillgångar

Kommunen ska inventera informationstillgångarna som finns i verksamheten. Kommunen ska säkerställa rätt och relevant nivå på informationssäkerhetsarbetet genom informationssäkerhetsklassning. Riktlinjer ska finnas för hur detta arbete ska genomföras.

Fysisk och teknisk säkerhet

Kommunen ska fastställa kraven på den fysiska och tekniska säkerheten i de egna systemen, i de system som hanteras via Göliska IT, via andra leverantörer och säkerställa att kraven uppfylls. En riktlinje ska finnas som beskriver fysisk och teknisk säkerhet.

Leverantörsrelationer

Kommunen ska fastställa de informationssäkerhetsrelaterade krav som ska användas vid upphandlingar och i avtal med leverantörer framförallt av IT-system och IT-drift.

Kommunen ska säkerställa skyddet för de informationstillgångar som leverantörer har åtkomst till genom att informationssäkerhetskrav ingår i leverantörsavtalen. Kommunen ska följa upp att leverantörerna lever upp till kraven på informationssäkerhet. Riktlinjer ska finnas som beskriver hur detta ska genomföras.

Hantering av informationssäkerhetsincidenter

Kommunen ska följa upp informationssäkerhetsarbetet genom att rapportera avvikelser, åtgärda informationssäkerhetsbrister och i förekommande fall rapportera incidenter till berörda myndigheter. Incidentrapportering krävs för att uppfylla vissa lagkrav. En rutin för avvikelsehantering och incidentrapportering ska finnas.

Efterlevnad

Efterlevnaden av informationssäkerhetsarbetet ska följas upp till exempel via internkontroll, revisioner och i ledningens förbättringsarbete.