Informationssäkerhet - riktlinjer

Antagen av …….
i ……. kommun
2019-xx-xx

Innehåll

Dokumentansvar
Ansvarig för dokumentet:
Ansvarig för revidering:
Gäller för: ……kommun
Gäller tillsvidare med revidering vid behov

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.) Därutöver finns verksamhetsspecifika krav på informationssäkerhet i bland annat i skollagen, socialtjänstlagen och hälso- och sjukvårdslagen.

Dataskyddsförordningen ställer krav på de informationstillgångar som hanterar 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.

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).

Samlad information och rådgivning finns att hämta på Informationssäkerhet.se.

4 Grundläggande krav och rekommendationer för informationssäkerhet

Grunden till dessa riktlinjer är hämtade från Sveriges kommuner och landsting (SKL) och Myndigheten för samhällsskydd och beredskap (MSB) som har gett rekommendationer till kommunerna avseende informationssäkerhet. Underlag har även hämtats från standarden och riktlinjerna för informationssäkerhet ISO 27001 och ISO 27002 samt från kraven i aktuell lagstiftning.

Skyddet för informationstillgångarna ska anpassas till en nivå som är rätt och relevant utifrån informationens skyddsvärde.

Följande områden säkerställs för att uppfylla grundläggande krav och rekommendationer.

4.1 Organisation av informationssäkerhetsarbetet

Kommunen ska ha en kompetent organisation med tydlig fördelning av ansvar för informationstillgångar och med relevanta roller för ledning och genomförande av ett systematiskt informationssäkerhetsarbete.

4.2 Personalsäkerhet

Samtliga chefer och medarbetare erbjuds relevant utbildning inom informationssäkerhet. Chefer ansvarar för att medarbetare har rätt behörighet och förutsättningar att hantera kommunens informationstillgångar.

Kommunen fastställer informationssäkerhetsrelaterade krav på bakgrundskontroll för befattningar som har hög behörighet i känsliga system, tillgång till känslig och skyddsvärd informationstillgång eller på annat sätt stor påverkansmöjlighet på informationssäkerheten.

Kommunen strävar efter en god säkerhetskultur i hela organisationen där det finns ett fungerande samspel mellan olika kompetenser inom säkerhet, informationssäkerhet, juridik och ledning. En säkerhetskultur som berör alla medarbetare.

4.3 Hantering av informationstillgångar

Kommunen samlar kunskap om vilka informationstillgångar som finns i verksamheten, fastställer de krav som informationstillgångarna ställer på informationssäkerheten och analyserar nuläget ur informationssäkerhetssynpunkt.

Kommunen säkerställer rätt och relevant informationssäkerhet genom att vidta organisatoriska och tekniska åtgärder.

4.4 Fysisk och teknisk säkerhet

Kommunen fastställer den fysiska och tekniska säkerheten i de egna systemen, i de system som hanteras via Göliska IT och via andra leverantörer.

Fysisk och teknisk säkerhet avser styrning av åtkomst, kryptering, fysisk och miljörelaterad säkerhet, driftssäkerhet, kommunikationssäkerhet, anskaffning, utveckling och underhåll av system samt informationssäkerhet avseende verksamhetens kontinuitet.

4.5 Leverantörsrelationer

Kommunen fastställer informationssäkerhetsrelaterade krav som används vid upphandlingar och i avtal med leverantörer framförallt av IT-system, IT-drift och liknande.

Kommunen säkerställer skyddet för de informationstillgångar som leverantörer har åtkomst till genom att informationssäkerhet ingår i leverantörsavtalen.

Kommunen följer upp att leverantörerna lever upp till kraven på informationssäkerhet som finns i leverantörsavtalen.

4.6 Hantering av informationssäkerhetsincidenter

Kommunen följer upp avvikelser i informationssäkerheten via incidentrapportering.

4.7 Efterlevnad

Informationssäkerhetsarbetet följs upp via internkontroll och revisioner.

5 Styrande dokument

För att säkerställa de grundläggande kraven och rekommendationerna ska styrdokument tas fram och integrerats i kommunens ledningssystem.