Program Plan **Policy** Riktlinje

Informationssäkerhetspolicy

Beslutad av: Kommunstyrelsen

Datum och paragraf: 2023-04-11, § 90

Revisionsdatum:

Dnr: 23KS48

ASKERSUNDS KOMMUN

Innehåll

1. Inledning

Information är en viktig tillgång och en förutsättning för att kommunen ska kunna bedriva verksamhet. Kommunens informationstillgångar måste därför hanteras på ett tillfredsställande sätt utifrån tre informationssäkerhetsaspekter:

- att information enbart är tillgänglig för behöriga (konfidentialitet)
- att information är korrekt, aktuell och fullständig (riktighet)
- att information är åtkomlig i rätt tid och användbar (tillgänglighet)

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, bland annat i skollagen, socialtjänstlagen och hälso- och sjukvårdslagen.

Dataskyddsförordningen ställer krav på hantering av personuppgifter.

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 regioner (SKR)
- Integritetsmyndigheten (IMY)
- Post- och telestyrelsen (PTS)

4. Policy

Denna policy utgör kommunens viljeinriktning för att hantera kommunens och dess bolags information på ett systematiskt och informationssäkert sätt.

Kommunens informationssäkerhetpolicy omfattar all information som kommunens verksamheter äger och hanterar.

Informationssäkerhetsarbetet ska vara en naturlig del av all verksamhet inom kommunen och dess bolag.

Det systematiska arbetet med informationssäkerhet ska utgå från gällande standarder för informationssäkerhet och integreras i kommunens och dess bolags ledningssystem. Lagar och förordningar utgör en grund för detta arbete, avtal ska följas och medborgarnas rättigheter och krav på utvecklad service införlivas.

Informationssäkerhetsarbetet ska underlätta arbetet med digitalisering samtidigt som kommunens, bolagens, medarbetarnas, kundernas och brukarnas information skyddas.

Ansvaret för informationssäkerheten följer verksamhetsansvaret. Alla chefer, medarbetare och förtroendevalda ansvarar för att denna policy följs när kommunens och dess bolags informationstillgångar hanteras.

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

4.1. Strategiska målsättningar

4.1.1. Systematiskt informationssäkerhetsarbete

Kommunens och dess bolags ledningssystem för informationssäkerhet ska uppfylla de grundläggande kraven på systematiskt informationssäkerhetsarbete enligt gällande standarder och ett arbetssätt som stödjer ständiga förbättringar ska tillämpas.

4.1.2. Organisation

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

4.1.3. Utbildning

Samtliga chefer och medarbetare ska genomgå utbildning. Förtroendevalda ska erbjudas utbildning. Informationssäkerhetssamordnaren samordnar utbildningar. Chefer ansvarar för att medarbetare har rätt behörighet och förutsättningar att i sitt arbete hantera kommunens och dess bolags informationstillgångar.

Kommunen och dess bolag ska fastställa informationssäkerhetsrelaterade krav på bakgrundskontroll för vissa befattningar.

Kommunen och dess bolag ska sträva efter en långsiktig säkerhetskultur i hela organisationen. En förutsättning för långsiktighet är styrande dokument, kompetent personal samt hantering av avvikelser och risker som underlag till ständiga förbättringar.

Det ska finnas ett utvecklande samarbete mellan olika kompetenser inom fysisk säkerhet, informationssäkerhet, IT, juridik, dokumenthantering och ledning.

4.1.4. Hantering av informationstillgångar

Kommunen och dess bolag ska ha kunskap om informationstillgångarna. En relevant nivå på informationssäkerhetsarbetet ska säkerställas genom informationssäkerhetsklassning.

4.1.5. Fysisk och teknisk säkerhet

Kommunen och dess bolag ska fastställa krav på fysisk och teknisk säkerhet i system och tjänster samt säkerställa att kraven uppfylls.

4.1.6. Leverantörsrelationer

Kommunen och dess bolag ska fastställa krav på informationssäkerhet vid upphandling och i avtal.

4.1.7. Uppföljning och rapportering

Kommunen och dess bolag ska följa upp informationssäkerhetsarbetet genom att rapportera avvikelser, åtgärda informationssäkerhetsbrister och i förekommande fall rapportera incidenter till berörda myndigheter. Uppföljning av informationssäkerhetsarbetet ska ske årligen till kommunstyrelsen. Särskilda skäl kan motivera ytterligare rapportering.