Eda kommun

Informationssäkerhetspolicy

– Styrdokument –

Eda kommun	Styrdokument	
	Dokumenttyp	Policy
	Beslutad av	Kommunfullmäktige 2017-05-17 § 73
	Dokumentansvarig	Informationssäkerhetssamordnare
	Reviderad av	Kommunfullmäktige 2019-07-03 § 93 Kommunfullmäktige 2021-12-15 § 167

Innehållsförteckning

Inledning

Information är en av kommunens mest kritiska resurser. Verksamheterna är beroende av information. Avbrott i tillgången och felaktig information kan orsaka allvarliga konsekvenser i verksamheten eller för enskilda individer.

Information behöver hanteras på ett säkert sätt. Detta för att skapa förtroende hos både anställda, förtroendevalda, brukare och allmänheten. Var och en som lämnar eller tar emot information ska kunna förlita sig på att den informationen är riktig, konfidentiell, tillgängligt och spårbar för rätt personer.

Policyn beskriver de övergripande principer som ska gälla för informationssäkerhetsarbetet i Eda kommun. Informationssäkerhetspolicyn gäller för hantering av all information, i alla dess former i kommunen inklusive bolag och för de som arbetar på uppdrag av kommunen. Det sistnämnda ska regleras genom avtal.
Informationssäkerhetsarbetet styrs av kommunens ledningssystem för informationssäkerhet utformat utifrån ISO/IEC 27000 och organisationens verksamhetskrav samt gällande författningar.

Ledningssystemet består av styrande dokument som utgörs av denna policy med tillhörande regler och eventuella rutiner samt tillämpningsanvisningar.

Arbetet med informationssäkerhet ska vara långsiktigt, systematiskt och kontinuerligt.

1.1 Begreppsförklaring

Informationstillgångar. Allt som innehåller information samt allt och alla som bär på information. T ex mobiltelefoner, verksamhetssystem och medarbetare.

Informationssäkerhet. Är den säkerhet som omfattar våra informationstillgångar och förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet.

Konfidentiell. Information som inte får nås eller avslöjas för någon obehörig. Oftast gäller det innehållet in en informationstillgång men ibland är även tillgångens existens hemlig.

Riktighet. Innebär att informationen inte får ändras av obehöriga, inte av misstag och inte på grund av en funktionsstörning.

Tillgänglighet. Innebär att informationen går att nyttjas av behörig användare när det behövs och så mycket det behövs.

Spårbarhet. Aktiviteter ska kunna härledas i efterhand. Vem som har utfört aktiviteten, vad som har skett samt var aktiviteten har utförts. I möjlig mån ska det även kunna spåras hur aktivitetens utfördes.

LIS. Ledningssystem för informationssäkerhet. En metod för att arbeta övergripande och systematiskt med informationssäkerhet. Metoden bygger

på standarderna i 27000-serien och rekommenderas av Myndigheten för samhällsskydd och beredskap.

Verksamhetssystem. I vissa fall även kallat informationssystem, är de system som insamlar, lagrar, bearbetar eller distribuerar och presenterar information.

1.2 Mål

Kommunens informationssäkerhetsarbete ska skydda informationen inom verksamheten mot yttre och inre hot. Skyddet ska vara anpassat till skyddsvärdet, risk och lagkrav och därigenom möjliggöra för kommunens verksamheter att uppnå sina mål. Följande mål är styrande för informationssäkerheten i kommunen

Säker och riskbaserad informationshantering

Informationstillgångar klassificeras och riskbedöms samt hanteras utifrån dess skyddsbehov, så att den är riktig och tillgänglig när den behövs och skyddas mot obehörig åtkomst. Det för att värna verksamhetens förmåga att utföra sitt uppdrag och skydda individer mot skada men lika viktigt är att värna integriteten för medborgarna.

Medborgarna ska känna trygghet i att kommunen omhändertar deras intressen avseende integritet och säkerhet i behandlingen av dennes uppgifter.

God informationssäkerhetskultur

Behovet av skydd av information bedöms och är en central del i arbetet på alla nivåer i verksamheten utifrån de risker och hot som finns mot informationen och medarbetare är medvetna om sitt ansvar som användare.

Effektiv incidenthantering

Kommunen har förmåga att hindra, hantera och lära av allvarliga informationssäkerhetsincidenter.

Robust informationshantering

Verksamheterna, IT och IT-infrastrukturen är riskbedömda och har planerat för vilka åtgärder som ska vidtas vid avbrott, störningar och kriser.

Informationssäkerhetsuppföljning

Kommunledningen och kommunstyrelsen ska informeras av särskild utsedda roller om informationssäkerhetsläget i Regionen samt vilka åtgärder som bör vidtas.

Handlingsplan

Informationssäkerhetsaspekter ska beaktas i handlingsplaner och verksamhetsplaner.

1.3 Syfte

Syftet med informationssäkerhetspolicyn är att beskriva hur kommunen ska uppnå en god informationssäkerhet.

2 Ansvar och organisation

Kommunfullmäktige fastställer den informationssäkerhetspolicy som ska gälla för Eda kommun.

Kommunstyrelsen ansvarar för att kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet utarbetas och hålls aktuella samt beslutar om regler för informationssäkerhet och följer upp handlingsplan med mätbara mål för informationssäkerhet.

Kommunstyrelsen ansvarar också för samordningen av informationssäkerhetsarbetet i kommunkoncernen.

Varje nämnd och bolagsstyrelse är, utifrån denna policy och kommunstyrelsens riktlinjer, ansvarig för informationssäkerheten inom sitt verksamhetsområde och ska inom ramen för kommunens ledningssystem där så är nödvändigt anta verksamhetsspecifika styrdokument för informationssäkerhet. Utskotten och bolagsstyrelse ska årligen planera och följa upp informationssäkerhetsarbetet och vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig säkerhet. Ansvaret för informationssäkerheten följer verksamhetsansvaret.

Alla medarbetare har ett ansvar för att säkerheten fungerar och följa uppställda säkerhetsregler. Detta gäller även när tillfällig personal eller extern aktör/ uppdragstagare anlitas. Den som upptäcker brister i informationssäkerheten ska uppmärksamma sin närmaste chef på det. Alla medarbetare ska rapportera händelser som kan göra att informationstillgångar utsätts för risker.

3 Arbetssätt och skyddsåtgärder

I den mån det är möjligt ska kommunen arbeta enligt LIS. LIS ska anpassas efter verksamheten.

Kommunens verksamheter ska arbeta med att identifiera informationstillgångar och dess flöden. Informationstillgångarna ska klassificeras enligt LIS.

Alla informationstillgångar ska ha en ägare. Informationsägaren ansvarar för klassificeringen och ställer de säkerhetskrav som behövs för att nå önskad säkerhet.

Alla verksamhetssystem ska ha en systemägare som ansvarar för att säkerhetskraven på systemet uppfylls.

Verksamheterna ska omvärldsbevaka och genomföra risk- och sårbarhetsanalyser vid införandet av nya verksamhetssystem och vid förändringar. Vid behov ska verksamheterna vidta nödvändiga åtgärder för att se till att informationstillgångarna har rätt skydd, vidare ska verksamheterna följa upp och dokumentera incidenter och vidtagna åtgärder kring dessa.

Kommunen ska ställa krav på informationssäkerhet vid upphandling, utveckling, användning och avveckling av verksamhetssystem. De krav som ställts ska även följas upp. Relevanta säkerhetskrav ska gälla vid såväl

intern som extern drift av verksamhetssystem. Viss säkerhetsklassad information kan kräva säkerhetsskyddad upphandling (SUA).

Verksamheterna ska arbeta med kontinuitetsplanering och ha beredskap för påfrestande situationer. Detta gäller även när externa aktörer för informationshantering anlitas. Samhällsviktiga verksamheter ska kunna upprätthållas på acceptabel nivå vid olika typer av störningar och krissituationer. Det är viktigt att alla har ett högt säkerhetsmedvetande och kritiskt ifrågasätter händelser som kan påverka informationssäkerheten.

Skyddsåtgärder ska vara kostnadseffektiva och stå i proportion till värdet av informationen och de negativa konsekvenser en otillräcklig säkerhet kan medföra.

Ansvariga enligt detta dokument ska följa upp att beslutade åtgärder är genomförda, att uppsatta mål är uppfyllda, att regler och riktlinjer följs samt att styrdokument vid behov revideras.

4 Uppfölja och revidera

Informationssäkerhetspolicyn ska revideras vart fjärde år eller vid behov. I samband med revideringen ska tillhörande riktlinjer och tillämpningsanvisningar revideras på motsvarande sätt.