Eda kommun



# Informationssäkerhetspolicy

– Styrdokument –

| Eda kommun | Styrdokument | |
|---|---|---|
| | **Dokumenttyp** | Policy |
| | **Beslutad av** | Kommunfullmäktige 2017-05-17 § 73 |
| | **Dokumentansvarig** | IT-chef |
| | **Reviderad av** | – |

# Innehållsförteckning

# 1 Inledning

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.

Arbetet med informationssäkerhet ska vara långsiktigt och kontinuerligt, omfatta alla delar av kommunens verksamheter och dess bolag. Policyn gäller alla de informationstillgångar som kommunen äger och hanterar. Personalen ska få fortlöpande utbildning för att förstå hur informationssäkerheten fungerar.

Informationssäkerhetspolicyn är inspirerad av den svenska standarden LIS (ledningssystem för informationssäkerhet) som rekommenderas av Myndigheten för samhällsskydd och beredskap.

Denna policy beskriver de övergripande principerna som gäller för informationssäkerhetsarbetet i Eda kommun.

## 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 obehörigen förändras, 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

Målet med kommunens informationssäkerhetspolicy är att upprätthålla önskad konfidentialitet, riktighet, tillgänglighet och spårbarhet för alla informationstillgångar.

### 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. 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. Utskotten och bolagsstyrelse ska löpande planera och följa upp informationssäkerhetsarbetet och vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll. Ansvaret för informationssäkerheten följer verksamhetsansvaret.

Alla medarbetare har ett ansvar för att säkerheten fungerar och följa uppställda säkerhetsregler. Det samma gäller när tillfällig personal eller extern aktör/ uppdragstagare anlitas. Den som upptäcker brister i informationssäkerheten måste uppmärksamma sin närmaste chef på det. Alla medarbetare ska kunna 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 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, förändringar

samt vid inträffade incidenter. Vid behov ska verksamheterna vidta nödvändiga åtgärder för att se till att informationstillgångarna har rätt skydd.

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 avbrott. 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.

Kommunen ska följa upp att beslutade åtgärder är genomförda, att uppsatta mål är uppfyllda, att regler och riktlinjer följs, att styrdokument vid behov revideras.

# 4 Uppföljning och revidera

Informationssäkerhetspolicyn ska revideras vart annat år eller vid behov. I samband med revideringen ska tillhörande riktlinjer och tillämpningsanvisningar revideras på motsvarande sätt. Informationssäkerhetspolicyn ska granskas och revideras enligt rekommendation i LIS.