Sunne kommun

Styrdokument

Informationssäkerhets-policy

SUNNE | VÄRMLAND

Dokumenttyp	Policy
Diarienummer	KS/2021:697
Beslutad av	Kommunfullmäktige 2018-05-07, § 57
Reviderad av	Kommunfullmäktige 2022-03-21, § 29
Dokumentansvarig	Informationssäkerhetsansvarig

Innehåll

1. Inledning

Information behöver hanteras på ett säkert sätt. Detta för att skapa förtroende hos både anställda, förtroendevalda, kunder och allmänheten. Var och en som lämnar eller tar emot information ska kunna förlita sig på att den informationen är;

- Riktig: att information är korrekt, aktuell och fullständig
- Konfidentiell: att information inte tillgängliggörs eller avslöjas till obehörig
- Tillgänglig: att information är åtkomlig och användbar av behörig
- Spårbar för rätt personer: att informationsbearbetning ska kunna härledas till vem och när

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 ledningssystem för informationssäkerhet (LIS), vars metod bygger på den svenska och internationella standardserien SS-ISO/IEC 27000. Metoden rekommenderas av Myndigheten för samhällsskydd och beredskap (MSB) och har sin utgångspunkt i en verksamhetsanpassad riskanalys där informationssäkerhetsarbetet följer en tydlig process.

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

1.1 Begreppsförklaring

Informationstillgångar - Allt som innehåller information samt allt och alla som bär på information. Till exempel 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 i 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.

Signalskydd - Kryptografiska funktioner, godkända av Försvarsmakten som används i syfte att förhindra obehörig insyn i och påverkan av telekommunikations- och IT-system.

LIS - Ledningssystem för informationssäkerhet. En metod för att arbeta övergripande och systematiskt med informationssäkerhet. Metoden bygger på standarderna i ISO 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 Sunne 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. Kommunstyrelse 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 verk-samhetsansvaret.

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 anpassas efter verksamheten.

- Varje behandling av personuppgifter ska ske i enlighet med gällande lagstiftning och hänsyn ska tas till den enskildes personliga integritet och rättigheter.
- Varje behandling ska följa Dataskyddsförordningens grundläggande principer: Laglighet, korrekthet och öppenhet, Ändamålsbegränsning, Uppgiftsminimering, Korrekthet, Lagringsminimering, Integritet och konfidentialitet, och Ansvarsskyldighet.

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 och en systemförvaltare, där systemägaren ansvarar för att säkerhetskraven på systemet uppfylls. Systemförvaltaren ska bistå användare av systemet i syfte att upprätthålla en hög informationssäkerhet. Systemägaren ansvarar för att skydd till information är anpassat och att man genomför riskanalyser med en regelbundenhet. Åtkomst och behörighet ska tilldelas formellt och vara baserat efter roll, behov och inte vara mer omfattande än det verkliga behovet. Det är av stor vikt att åtkomst och behörigheter avslutas vid avslut av tjänst eller byte av arbetsuppgifter och det ligger på systemägarens ansvar att tillse att det sker.

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).

Signalskyddet och dess funktioner utförs endast av säkerhetsklassad personal i för ändamålet avsett utrymme och kontroll av efterlevnaden sker av utsedd myndighet.

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.

Kommunstyrelsen ska följa upp att beslutade åtgärder är genomförda, att uppsatta mål är uppfyllda, att regler och riktlinjer följs, att styrdokument vid behov revideras. Informationssäkerhetssamordnare ska en gång per år rapportera läge och status gällande informationssäkerhet till kommunstyrelsen och till kommunledningsgruppen.

Hantering av undantag från antagen policy ska vara förankrade i kommunledningsgruppen och skyndsamt rapporteras till kommunstyrelsen. Incidenter ska omgående rapporteras till informationsägare och systemägare och hanteras skyndsamt och prioriterat. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.

4. Uppföljning och revidering

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.