Sunne kommun

Styrdokument

Riktlinje för incidenthantering

SUNNE | VÄRMLAND

Dokumenttyp	Riktlinje
Diarienummer	KS/2024:572
Beslutad av	Kommunstyrelsen 2025-02-06, § 12
Reviderad av	
Dokumentansvarig	Samordningsgrupp för dataskydd och informationssäkerhet

Innehåll

1. Inledning

Denna riktlinje gäller för hela Sunne kommun med dess bolag, alla anställda, förtroendevalda och andra som har behörighet att använda kommunens resurser för IT-kommunikation.

I enlighet med Sunne kommuns policy för informationssäkerhet ska Sunne kommun arbeta systematiskt och riskorienterat med informationssäkerhet. En viktig del av det riskorienterade arbetet är att hantera incidenter gällande informationssäkerhet, personuppgifter och IT-säkerhet.

2. Syfte och mål

2.1 Syfte med riktlinjen

Riktlinjen har till syfte att beskriva hur incidenter ska hanteras och hur rapportering av incidenter ska ske i Sunne kommuns verksamheter och bolag. Riktlinjen har också till syfte att fastställa roller och ansvar i och med incidenthantering.

2.2 Mål

Att arbeta efter en kommungemensam modell när det gäller att förebygga, upptäcka och hantera incidenter.

3. Övriga styrdokument, lagar och förordningar av relevans för riktlinjen

- Policy för informationssäkerhet
- Riktlinje för Organisation och ansvar för dataskyddsarbetet i Sunne kommun
- Dataskyddsförordningen
- Dataskyddslagen
- ISO 27000-serien
- Säkerhetsskyddslagen (2018:585)
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-direktivet)

4. Ansvar och organisation

4.1 Organisation

Kommunfullmäktige fastställer policy för incidenthantering som ska gälla för Sunne kommun. Kommunstyrelsen ansvarar för att kommunens riktlinje för incidenthantering samt att program och planer för denna riktlinje utarbetas och hålls aktuella.

Varje nämnd och bolagsstyrelse är, utifrån denna riktlinje, ansvarig för incidenthantering inom sitt verksamhetsområde. Ansvaret för incidenthantering följer verksamhetsansvaret. Alla medarbetare har ett ansvar att följa uppställda styrdokument. Det samma gäller när tillfällig personal eller extern aktör/uppdragstagare anlitas.

4.2 Funktion och ansvar

Tabell för funktion och ansvar:

Funktion	Ansvarar för
Samordningsgrupp för dataskydd och informationssäkerhet	Riktlinjer och rutiner gällande incidenthantering
Dataskyddsombud Samordningsgrupp för dataskydd och informationssäkerhet	Ta emot och bedöma personuppgiftsincidenter
Dataskyddssamordnare	Anmäla till Integritetsskyddsmyndigheten (IMY) efter beslut av ansvarig chef enligt delegationsordningen
Dataskyddsamordnare och informationssäkerhetssamordnare	Registrera och utreda personuppgiftsincident och koppla informationstillgång och behandling, skriva fram förslag på åtgärder på kort och lång sikt samt följa upp åtgärder
Ansvarig chef	Beslutar om åtgärder på kort och lång sikt i samråd med Dataskyddsamordnare och informationssäkerhetssamordnare
IT-chef	Ta emot och bedöma IT-incidenter, eventuellt anmäla vidare till Myndigheten för samhällsskydd och beredskap (MSB). Skriva fram åtgärdsrapport.
Styrgrupp för dataskydd och informationssäkerhet (kommunledningsgruppen)	Ansvarar för att strategiskt styra, stödja och leda arbetet med informationssäkerhet och dataskydd. Ansvarar för att besluta om genomförande av övergripande utbildning. Vara vägledande vid allvarligare incidenter.

5. Riktlinje för incidenthanteringen

5.1 Anmälan av incidenter

- Samtliga medarbetare har ett ansvar att anmäla incidenter.
  En medarbetare ska:
  - ha kännedom om vad en incident är
  - veta hur incidenten ska anmälas
- Att anmäla en incident ska vara lätt och det ska tydligt framgå att det alltid är själva incidenten som anmäls och inte den som anmäler.
- En incident ska alltid anmälas. För att tidigt kunna påbörja riskminimering och hantera incidenten ska anmälan påbörjas även om all information inte finns att tillgå. Komplettering av anmälan ska ske allt eftersom ny information finns tillgänglig.
- Det ska finnas tydliga ingångar på Sunne kommuns intranät för anmälan med instruktioner hur anmälan görs och vad som händer efter att anmälan är gjord.

5.2 Dokumentation av inträffade incidenter

- Incidenter ska dokumenteras. Syftet med att dokumentera incidenter är att:
  - skapa förutsättningar för att vidta rätt skyddsåtgärder
  - utveckla förmågan att förebygga, upptäcka och hantera incidenter

5.3 Uppföljning och anmälningsplikt

- Incidenter och åtgärder ska följas upp och fungera som ett lärtillfälle för verksamheterna.
- Incidenter som omfattas av anmälningsplikt enligt gällande lagar, förordningar eller föreskrifter ska anmälas till tillsynsmyndighet.

5.4 Rutinbeskrivningar

- Det ska finnas upprättade rutinbeskrivningar med tydlig ansvarsfördelning och rollbeskrivning för respektive incidentkategori.

6. Begreppsindikationer

Samlingsbegreppet incident inbegriper IT-incidenter, informationssäkerhetsincidenter, IT-säkerhetsincidenter och personuppgiftsincidenter, vilka kommer att redogöras för nedan. Incidenter kan vara IT-incident, informationssäkerhetsincident, IT-säkerhetsincident, en personuppgiftsincident eller en kombination av dessa.

6.1 IT-incidenter

En IT-incident är en oönskad och oplanerad störning i mjuk- eller hårdvara som kan få eller har fått negativa konsekvenser för verksamheten, enskild individ eller tredje part. En IT-

incident kan antingen bero på ett medvetet eller omedvetet agerande, men till skillnad från en IT-säkerhetsincident beror en IT-incident aldrig på ett antagonistiskt angrepp. Exempel på IT-incidenter är störningar i driftsmiljön, dataförlust eller dataläckage.

6.2 Informationssäkerhetsincidenter

Informationssäkerhetsincidenter är händelser som påverkar, eller kan komma att påverka, säkerheten negativt för Sunne kommuns informationstillgångar. Den gemensamma nämnaren är att informationssäkerheten hotas genom till exempel obehörig åtkomst till information, obehörig hantering av information, felaktig information eller brist på tillgång till information.

Exempel på informationssäkerhetsincidenter kan vara att obehörig tar del av ett samtal i offentlig miljö, att fysiska dokument lämnas utan uppsikt eller obehörig åtkomst till digital information.

6.3 IT-säkerhetsincident

En IT-säkerhetsincident är ett avsiktligt angrepp som påverkar säkerheten negativt för våra informationstillgångar. Exempel på IT-säkerhetsincidenter kan vara kapad inloggning, dataintrång, angrepp med skadlig kod (virus på dator), bedrägeriförsök via e-post.

6.4 Personuppgiftsincident

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Den kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. Exempel på personuppgiftsincidenter är felaktigt utskick av personuppgifter eller att uppgifter i våra verksamhetssystem inte finns tillgängliga.

7. Uppföljning och revidering

Riktlinje för incidenthantering ska revideras vart annat år eller vid behov. I samband med revideringen ska tillhörande riktlinjer och rutiner revideras på motsvarande sätt.