Policy

Styrdokument

Policy för informations-säkerhet, It-säkerhet och dataskydd

Antaget av: Kommunfullmäktige
Datum: 2024-09-26
Gäller från och med: 2024-09-26
Ansvar uppföljning/uppdatering: Utvecklingschef
Gäller till och med: 2028

ULRICEHAMNS KOMMUN

Våra styrdokument

[Normerande]

Vision – Överordnad, anger riktning för övriga dokument
Policy – Vår hållning, övergripande
Riktlinjer – Rekommenderade sätt att agera
Regler – Absoluta gränser och ska-krav

[Aktiverande]

Strategi – Avgörande vägval och strategiområden
Program – Avgörande vägval och programområden
Plan – Uppdrag, tidsram och ansvar

Innehåll

1 Bakgrund

Information är en viktig tillgång för kommunens alla verksamheter inklusive de kommunala bolagen och är av betydande värde för de vi är till för. Kommunens informationstillgångar består av all information som finns hos kommunen, inkommer till kommunen eller som upprättas av kommunen, oavsett var den förvaras och om den är digital, pappersbunden eller muntlig. En del av vår information består av personuppgifter.

2 Syfte

För att trygga informationsförsörjningen och värna om den personlig integriteten ska kommunen bedriva ett långsiktigt och systematiskt informationssäkerhets-, It-säkerhets- och dataskyddsarbete som bygger på etablerade standarder.

Målsättningen är att upprätthålla rätt nivå på skydd av informationstillgångarna avseende **tillgänglighet** (att information är åtkomlig för behörig person vid rätt tillfälle), **riktighet** (att information är tillförlitlig, korrekt och fullständig) och **konfidentialitet** (att information skyddas för obehörig insyn).

Dataskyddsarbetets målsättning, utöver vad som gäller för informationssäkerhet, är att de personuppgifter som kommunen hanterar ska behandlas i enlighet med de grundläggande dataskyddsprinciperna i dataskyddsförordningen och i enlighet med övriga dataskyddsregler. Informationssäkerhets-, It-säkerhets- och dataskyddsarbetet samordnas då ett gott informationssäkerhets- och It-säkerhetsarbete är en förutsättning för att följa dataskyddslagstiftningen.

Strategiska målsättningar för informationssäkerhetsarbetet

- Personal har kunskap om gällande lagar/regler/föreskrifter och rutiner som gäller för hantering av information och personuppgifter och kan omsätta dessa i praktiken
- Verksamheterna värderar sina informationstillgångar utifrån en gemensam klassificeringsstruktur och vidtar lämpliga skyddsåtgärder
- Verksamheterna dokumenterar och håller samman arbetet med informationssäkerhet och dataskydd i systemförvaltningsplanen utifrån kommunens förvaltningsmodell

3 Roller och ansvar

Kommunfullmäktige är ytterst ansvarig för informationssäkerhets-, It-säkerhets- och dataskyddsarbetet och uttrycker sin viljeinriktning i denna policy.

Kommunstyrelsen ansvarar för att samordna och följa upp kommunens informationssäkerhets-, It-säkerhets- och dataskyddsarbete. Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta och följa upp riktlinjer för informationssäkerhet, It-säkerhet och dataskydd.

Nämnder med förvaltning och kommunala bolag ansvarar för informationsägarskapet inom ramen för sina verksamheter. Informationsägaren har det yttersta ansvaret för sin information och avgör vilken information som får hanteras, hur den ska hanteras och av vem den får hanteras. Dataskyddsförordningens stadgar pekar ut att ansvaret är knutet till den som är personuppgiftsansvarig. Det innebär att det är kommunens nämnder som själva har det yttersta ansvaret för att personuppgiftsbehandlingar i varje enskilt fall utförs i enlighet med förordningens regler och principer.

Policyn för informationssäkerhet, It-säkerhet och dataskydd gäller för alla informationstillgångar och personuppgiftsbehandlingar i alla verksamheter inom kommunen och de kommunala bolagen. Policyn gäller för samtliga aktörer som kan komma att hantera kommunens information och personuppgifter.

De som hanterar information och personuppgifter ska ha kunskap om det regelverk som gäller för hur informationen och personuppgifterna får hanteras och har själva ett ansvar för att informationssäkerheten och dataskyddet upprätthålls. Vid upptäckt av incident eller brister ska incidentrapportering ske enligt rutin.