Informationssäkerhetspolicy

Dokumenttyp: Policy

Antaget av: Kommunfullmäktige

Antagen: 2018-04-26

Giltighetstid: Tillsvidare

Ronneby kommun

Ronneby.se

Diarienummer: KS 2017/209, KS 2022/298

Ansvarig för dokumentet: Informationssäkerhetsansvarig

Tidpunkt för senaste aktualitetsprövning:

Tidpunkt för senaste revidering: KF 2022-09-29 § 162

Relaterade styrdokument:

Sökord: Policy, styrdokument, kommunövergripande, dataskydd, informationssäkerhet

1. Inledning

Information är en värdefull resurs för Ronneby kommun. Alla verksamheter är beroende av tillförlitlig information. Obehörigt tillträde till information och informationsavbrott kan ge allvarliga och långtgående konsekvenser. Information tillgängliggörs i den kommunala verksamheten på många olika sätt. För att upprätthålla ett lämpligt skydd mot oförutsedda händelser måste det vara tydligt för alla hur information ska hanteras.

2. Omfattning

Denna policy gäller vid hantering av information i Ronneby kommuns verksamhet. Med Ronneby kommun avses i denna policy kommunfullmäktige, kommunstyrelsen, samtliga nämnder samt i tillämpliga delar de av kommunen helägda aktiebolagen.

3. Syfte

Arbete med informationssäkerhet syftar till att skydda information inom organisationen. Utbyte av information ska ske på ett säkert sätt. Alla ska vara medvetna om de risker som är förknippade med hantering av information, oavsett hur informationen tillgängliggörs.

Informationssäkerhetspolicyn är ett strategiskt dokument som ska synliggöra kommunfullmäktiges viljeriktning för allt informationssäkerhetsarbete i Ronneby kommun.

4. Definitioner

Arbetet med informationssäkerhet innebär att värdera och klassa information efter sin känslighet. Med hjälp av administrativa och tekniska skyddsåtgärder ska det säkerställas att informationen skyddas genom att:

- den alltid finns när vi behöver den (tillgänglighet)
- vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet)
- endast behöriga personer får ta del av den (konfidentialitet)
- identifiera och autentisera användare, samt loggning av relevanta händelser (spårbarhet)

Med informationstillgångar avses all information, oavsett om den behandlas manuellt eller automatiserat och oberoende dess form eller i vilken miljö den förekommer. Det är betydelsen av informationen som ska vara styrande, inte vilket system den ligger i, vilken organisation som behandlar informationen eller den teknik som tillgängliggör den.

5. Målsättning

Det ska finnas en bred förståelse för vikten av god informationssäkerhet. Informationssäkerhet ska vara en del av det dagliga arbetet för att säkerställa att informationstillgångar hanteras på ett sådant sätt att legala, verksamhetsmässiga och etiska ändamål upprätthålls. Kommunens verksamhet ska utformas i enlighet med dataskyddsförordningen (GDPR).

Kommunen ska verka för införande av ett ledningssystem för informationssäkerhet.

Medborgare, företagare och övriga intressenter ska känna sig trygga i kontakten med Ronneby kommun och vara säkra på att personuppgifter och andra informationstillgångar hanteras på ett tillförlitligt sätt.

6. Ansvar

Kommunfullmäktige är kommunens högsta beslutande organ och ansvarar för fastställande av kommunens informationssäkerhetspolicy.

Kommunstyrelsen leder och samordnar kommunens informationssäkerhetsarbete.

Kommunstyrelsen, nämnderna och bolagen har fullmäktiges uppdrag att sörja för att informationssäkerhetsarbetet inom sitt respektive verksamhetsområde sköts på ett så effektivt sätt som möjligt.

Chefer på alla nivåer har ett särskilt ansvar att informera om informationssäkerhetspolicyn och dess tillämpning.

Samtliga som hanterar information i kommunens verksamhet har därför ett ansvar att följa de informationssäkerhetsriktlinjer och instruktioner som finns samt att agera säkerhetsmedvetet.

7. Roller och organisation

Följande roller är centrala för det strategiska och operativa informationssäkerhetsarbetet:

Kommundirektör	Har det övergripande ansvaret för informationssäkerheten i den kommunala förvaltningen och utser systemägare för respektive informationssystem.
VD	Har det övergripande ansvaret för informationssäkerheten i den helägda kommunala bolaget och utser systemägare för respektive informationssystem.
Informationssäkerhets-ansvarig	Har i uppgift att inom ramen för kommunstyrelsens samordningsansvar, samordna kommunens informationssäkerhetsarbete. Samordnar informationssäkerhetsgruppens verksamhet.
Informationssäkerhets-kontaktperson	Kontaktperson på förvaltningsnivå i informationssäkerhetsfrågor. Ingår i kommunens informationssäkerhetsgrupp. Verksam i det löpande arbetet på förvaltningen.
Dataskyddsgrupp	Forum för att samordna och effektivisera hanteringen av dataskydds- och informationssäkerhetsfrågor i kommunen.
IT-chef	Ansvarar för att säkerställa kommunens behov av säker IT-drift.

Dataskyddsombud	Utövar tillsyn över kommunens behandling av personuppgifter, lämnar råd och stöd i dataskyddsfrågor m.m. Dataskyddsombudets uppgifter följer av art. 39 dataskyddsförordningen.
Personuppgiftsansvarig	Kommunstyrelsen, varje nämnd och varje bolag.
Systemägare	Har ett övergripande ansvar för informationstillgångar i systemet. Rollen förutsätter ett övergripande förvaltnings- och budgetansvar med direkt inflytande över förvaltningens strategiska och operativa verksamhet.
Systemförvaltare	Ansvarar för hantering av informationstillgångar i ett eller flera system. Ansvarar för löpande operativt arbete och har expertkunskaper i systemet. Utses av systemägare.
Systemadministratör	Användare med utökad behörighet i digitala system. Utses av systemförvaltare.

8. Tillämpning

Informationssäkerhetspolicyn konkretiseras genom av kommunstyrelsen framtagna riktlinjer för kommunens informationssäkerhetsarbete.

9. Uppföljning och revidering

Informationssäkerhet är ingen statisk verksamhet, uppföljning ska därför ske löpande och regelbundet. Revidering av denna policy ska ske vid behov, kommunstyrelsen ansvarar dock för att policyn genomgår en översyn och fastställs varje mandatperiod men minst vart fjärde år.