

Informationssäkerhetspolicy

Sorsele kommun

Dokumenttyp: Policy

Dokumentnamn: Informationssäkerhetspolicy Sorsele kommun

Beslutat datum: 2023-09-25 § 112

Gäller från datum: 2023-09-25

Beslutat av: Kommunfullmäktige

Ansvarig: Enhetschef-IT

Diarienummer: 2023/382-167

1. Informationssäkerhet

Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån från fyra aspekter:

- **Konfidentialitet:** Att information inte tillgängliggörs eller delges obehörig.
- **Riktighet:** Informationen ska vara tillförlitlig, korrekt och fullständig. Informationen ska skyddas mot oönskad eller obehörig förändring.
- **Spårbarhet:** Det ska i efterhand vara möjligt att se vem som har skapat, läst, ändrat eller raderat information. Nivån på spårbarhet bestäms vid informationssäkerhetsklassificeringen.
- **Tillgänglighet:** Informationen ska vara tillgänglig, för den som är behörig att ta del av den, i förväntad utsträckning och inom önskad tid.

Informationssäkerheten är en integrerad del i vår verksamhet. Alla som hanterar information har ett ansvar att upprätthålla informationssäkerheten. Det följer också med ett ansvar för chefer på alla nivåer att informera om vikten av verkningsfull ledning av informationssäkerhetsarbetet och att kraven i styrdokumenterna uppfylls.

Policyn ska vidare konkretiseras i ett antal styrdokument som innehåller mer detaljerad information och regler för hur arbetet med informationssäkerhet utförs i organisationen.

2. Syfte

Informationssäkerhetspolicyns syfte är att fungera som ett ramverk för kommunens arbete med informationssäkerhet utifrån målformulering, ansvar och uppföljning.

Genom utveckling av informationssäkerhetsarbetet i organisationen minimerar vi konsekvenser och risker inför angrepp och hot. Ytterst för att minimera att angrepp kan resultera i att samhällsviktig infrastruktur och funktioner slås ut.

Vidare genereras flertalet nyttor genom arbetet med att kartlägga informationsflöden och informationsprocesser och därigenom ge förbättrad styrning och ledning samt resultatuppföljning.

3. Mål

Målet med Sorsele kommuns informationssäkerhetsarbete är att informationen som hanteras inom verksamheterna följer grundprinciperna om tillgänglighet, riktighet, spårbarhet och konfidentialitet.

Konkretiserat innebär det att Sorsele kommun ska nå och upprätthålla en nivå inom informationssäkerhetsarbetet som:

- efterlever nationellt antagna lagar, förordningar, föreskrifter samt avtal,
- efterlever internationella standarderna inom ISO-27000 serien.,
- skyddar informationstillgångar i nivå med dess värde samt i relation till eventuella konsekvenser,
- bedriver ett systematiskt och kontinuerligt informationssäkerhetsarbete, vilket innebär återkommande uppföljning och förbättringar i ledningssystemet.

4. Roller och ansvar för informationssäkerhetsarbetet

Nedan beskrivs övergripande informationssäkerhetsansvar för rollerna:

Kommunfullmäktige

Beslutar om vilken informationssäkerhetspolicy som ska gälla för kommunen.

Kommunstyrelsen

Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhetsarbete. Genom mål och resultatuppföljning, intern kontroll och revision, fattar de nödvändiga beslut och tilldelar tillräckliga resurser för att informationssäkerhetsarbetet skall nå förväntat resultat. Kommunstyrelsen fastställer riktlinjer för informationssäkerhetsarbetet.

Kommunchef

Är sammankallande för kommunledningsgruppen. Har det ytterst operativa ansvaret och fattar de avgörande besluten om hur informationssäkerhetsarbetet ska bedrivas.

Kommunledningsgrupp

Kommunledningsgruppen har operativt ansvar för kommunens informationssäkerhetsarbete, att lämpliga roller finns på plats inom organisationen och att informationssäkerhetssamordnare samt övrig personal har den kunskap och de resurser som krävs för att säkerställa att kommunens mål kring

informationssäkerhet nås. Efterlevnaden av informationssäkerhetsarbetet ska följas upp och årligen rapporteras till kommunstyrelsen.

Informationssäkerhetssamordnare

Har det övergripande ansvaret för att utveckla och samordna arbetet med informationssäkerhet i kommunen. Stödfunktion för ledning och verksamheter.

Verksamhetschef

Varje verksamhetschef är ansvarig för informationssäkerheten inom sin verksamhet. Varje verksamhetschef ska upprätta de verksamhetsspecifika rutiner som behövs för att säkerställa att denna policy, inklusive tillhörande riktlinjer, är lämpliga, väl kända och följs inom den egna verksamheten.

Informationsägare

Är den som bestämmer ändamålen för behandlingen och hanteringen av informationen. Informationsägaren äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids.

Systemägare

Ansvarar övergripande för respektive system och dess användning, för säkerheten i informationstillgångar, klassning av informationstillgångar samt för genomförande av åtgärder för att minimera risk.

Systemförvaltare

Har det dagliga helhetsansvaret för ett system. Systemförvaltaren fungerar i hög grad som systemägarens utförare och ser till att systemets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.

Systemadministratör

Denne innehar systemkompetens samt ansvarar, tillsammans med systemägare och systemförvaltare, för att den dagliga driften och säkerheten upprätthålls.

Enhetschef-IT

Har ett särskilt ansvar för den tekniska IT-säkerheten i organisationen.

Kommunens medarbetare

Kommunens medarbetare ansvarar för att följa denna policy samt tillhörande riktlinjer och andra styrande dokument inom området. Det är varje medarbetares

ansvar att känna till vilka regler som gäller för informationssäkerhet samt att rapportera informationssäkerhetsincidenter enligt gällande rutin.

5. Hantering av informationssäkerhetsincidenter

Kommunen ska följa upp informationssäkerhetsarbetet genom att rapportera avvikelser, åtgärda informationssäkerhetsbrister och i förekommande fall rapportera incidenter till berörda myndigheter.

6. Uppföljning och efterlevnad

Kommunen ska följa lagar, författningar, avtalsförpliktelser, samt andra säkerhetskrav.

Chefer inom kommunen ska säkerställa att alla säkerhetsrutiner inom deras respektive ansvarsområde utförs korrekt för att uppnå efterlevnad av kommunens informationssäkerhetsarbete.

Efterlevnaden av informationssäkerhetsarbetet ska följas upp och årligen rapporteras till kommunstyrelsen via internkontroll.