

Informationssäkerhetspolicy

Framtagen av: Anders Kopp

Datum: 2024-08-12

Version: 2.0



LILLA EDETS
KOMMUN



Bakgrund

En av kommunens värdefullaste tillgångar är information. Information finns i alla kommunens verksamheter och rör exempelvis våra medborgare och anställda, våra kunder och brukare, våra elever, vår ekonomi och mycket annat.

Det är av avgörande betydelse för oss att skydda denna information så att enbart rätt personer har tillgång till korrekt information när den behövs.

Med information eller informationstillgång avses all information i alla dess former. Detta oavsett hur den lagras, transporteras, bearbetas eller kommuniceras. Information är mediaoberoende och kan till exempel vara i form av text, ljud, bilder och film, och kan hanteras digitalt, på papper eller när vi pratar.

Informationssäkerhet handlar om just det – att säkerställa rätt skydd för att ständigt ha relevant nivå av säkerhet.

Informationssäkerheten omfattar kommunens alla informationstillgångar utan undantag.

Informationssäkerhetsarbete innefattar allt kommunens medarbetare gör för att säkerställa att informationstillgångarna är skyddade.

Definition av informationssäkerhet

Informationssäkerhet handlar om hur vi skyddar våra informationstillgångar. Det finns lagar som ska uppfyllas samtidigt finns behov av tekniska lösningar för att möta och motverka den hotbild som finns. Tyvärr finns många hot mot våra informationstillgångar som behöver hanteras, allt ifrån medvetna angreppsförsök till oavsiktlig åverkan. Samtidigt behöver vi möta verksamhetens krav på tillgänglighet och smidighet. Den faktiska säkerhetsnivån blir en avvägning mellan ett antal, ibland motsägelsefulla, krav.

Skydd av personuppgifter som följer av Dataskyddsförordningen, GDPR, kallas vanligen för Dataskydd. Viktigt att notera att även om en personuppgift skyddas väl, så måste ändå ett korrekt ändamål för den behandlingen finnas annars får vi inte hantera personuppgiften.

Informationssäkerhet handlar om:

Konfidentialitet - att åtkomst till informationen kan begränsas så att den inte görs tillgänglig eller avslöjas för obehörig.

Riktighet - att informationen ska vara tillförlitlig, korrekt och fullständig

Tillgänglighet - att informationen ska vara tillgänglig och kunna nyttjas efter behov och i förväntad utsträckning.

En informationstillgång klassificeras utifrån konsekvensen om någon av ovanstående punkter inte uppfylls. Exempelvis:



- Vad blir konsekvensen om informationen avslöjas för obehörig eller om obehöriga kan komma åt de system där informationen lagras?
- Vad blir konsekvensen om vi inte kan lita på informationen?
- Vad blir konsekvensen om informationen inte går att komma åt när den behövs?

Utifrån hur allvarlig konsekvensen blir för en viss informationstillgång följer hur den behöver skyddas.

Det finns lagar med krav på hur vi hanterar vår information, exempelvis

- Arkivlag
- Dataskyddsförordningen, GDPR
- NIS-direktivet
- NIS2-direktivet (Cybersäkerhetslagen)
- Offentlighets- och sekretesslagen
- Patientdatalagen
- Socialtjänstlagen

Det finns etablerade standarder för informationssäkerhet, bland annat

- SS-ISO/IEC 27000-serien

Metodstöd för arbete med informationssäkerhet, baserat på dessa standarder, finns från bland annat

- MSB - Myndigheten för Samhällsskydd och Beredskap
- SKR – Sveriges Kommuner och Regioner

Syfte med informationssäkerhetspolicy

Informationssäkerhetspolicyen redovisar ledningens mål för informationssäkerhet och viljeinriktning att följa legala krav, standarder och metodstöd i det arbetet.

Policyn konkretiseras i Riktlinjer för informations- och IT-säkerhet som beslutas av Kommunstyrelsen

Regler och anvisningar i anslutning till detta beslutas av Kommunchefen.

Mål med informationssäkerhetsarbetet

Kommunens mål med informationssäkerhetsarbetet är att:

- Alla informationstillgångar ska ha ett relevant skydd.
- Lagar, förordningar och föreskrifter ska vara kända och följas.
- Informationssäkerhetsarbete ska ske löpande, metodiskt och riskbaserat i syfte att ständigt förbättras.
- Risker utvärderas löpande och åtgärdsplaner upprättas och genomförs.
- Personal ska ha relevant kunskap om informationssäkerhet.
- Krishanteringsförmågan upprätthålls och kontinuitetsplaner underhålls löpande.
- Rutin för hantering av informationssäkerhetsincident finns och följs.



- Rutin för att hantera avvikelser och undantag finns och följs.
- Informationssäkerhetsarbete ska dokumenteras
- Personal ska vara medvetna om hur de ska medverka i informationssäkerhetsarbetet.

Roller och ansvar

Informationssäkerhet är en integrerad del av den ordinarie verksamheten.

Kommunfullmäktige fastställer policy för informationssäkerhet.

Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhet och dess policy och fastställer efterföljande riktlinjer för informations- och IT-säkerhet.

Kommunchefen har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den fastställda informationssäkerhetspolicyn samt fastställer kommunövergripande regler och anvisningar.

Varje **nämnd** är ansvarig för att resursfördelning för informationssäkerhet sker på ett lämpligt sätt inom sitt verksamhetsområde.

Digitaliseringschefen har det operativa ansvaret för samordning av informationssäkerhetsarbetet.

Samtliga chefer ansvarar för informationssäkerhet och dataskydd inom sin verksamhet.

Samtliga medarbetare, oavsett roll, förväntas bidra till att alla informationstillgångar skyddas i enlighet med denna policy och de riktlinjer och regler som följer av denna. Om överträdelser sker, kommer arbetsrättsliga åtgärder att övervägas, vilket kan innebära att medarbetare erhåller disciplinär åtgärd eller skiljs från sin anställning.

Revidering och uppföljning

Uppföljning är en viktig del av informationssäkerhetsarbetet. Informationssäkerhetspolicyn följs upp i sin helhet varje mandatperiod och revideras vid behov.