Informationssäkerhetspolicy

Framtagen av: Kim Borg

Datum: 2021-02-15

Version: 1.0

Antagen av KF 2021-04-12

LILLA EDETS KOMMUN

Bakgrund

Grundläggande fokus för Lilla Edets kommuns informationssäkerhetspolicy är bland annat det pågående arbete som Myndigheten för samhällsskydd och beredskap (MSB) driver inom området och den vägledning som myndigheten tagit fram för kommunernas eget arbete kring informationssäkerhet.

Ytterligare krav på att stärka kommunernas informationssäkerhet kom i samband med NIS lagen.

(Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster) Detta har direkt påverkan på kommunens verksamhet inom flera områden.

Syftet med NIS-lagen

1 § Syftet med denna lag är att uppnå en hög nivå på säkerheten i nätverk och informationssystem för

1. Samhällsviktiga tjänster inom sektorerna

   - Energi
   - Transport
   - Bankverksamhet
   - Finansmarknadsinfrastruktur
   - Hälso- och sjukvård
   - Leverans och distribution av dricksvatten
   - Digital infrastruktur, och

2. Digitala tjänster

Myndigheten för samhällsskydd och beredskap (MSB) beskriver de grundläggande anledningarna till att myndigheten uppmanar kommunen att ta ansvar och följa lagen på följande sätt:

Sveriges kommuner hanterar en betydande del av samhällets tjänster och kommunernas informationsförsörjning är därför en kritisk del i samhällets informationssäkerhet. För att kunna säkerställa en tillräcklig nivå av informationssäkerhet i en kommuns olika förvaltningar och bolag är det av stor betydelse att informationssäkerhetsarbetet bedrivs metodiskt och långsiktigt.

Syftet med denna vägledning är att på ett konkret sätt stödja kommuner att bedriva ett sådant arbete. Myndigheten för samhällsskydd och beredskap (MSB) har givit ut föreskrifter om statliga myndigheters informationssäkerhet. Föreskrifterna pekar på att myndigheterna ska följa de internationella standarderna på området, ISO/IEC 27001 och ISO/IEC 27002. Dessa föreskrifter är endast bindande för statliga myndigheter men det finns stora vinster med att också kommuner arbetar med informationssäkerhet på samma systematiska sätt.

Utvecklingen inom e-förvaltning kommer att kräva att kommuner, myndigheter och landsting samverkar än mer. Om alla parter arbetar efter gällande standarder på området kommer det att

finnas en ömsesidig förståelse vad gäller säkerhetsfrågor och ett gemensamt språk kring detta. Det skapar exempelvis ökad effektivitet, högre säkerhetsmedvetande och minskade kostnader.

(MSB, Kommunens informationssäkerhet - en vägledning)

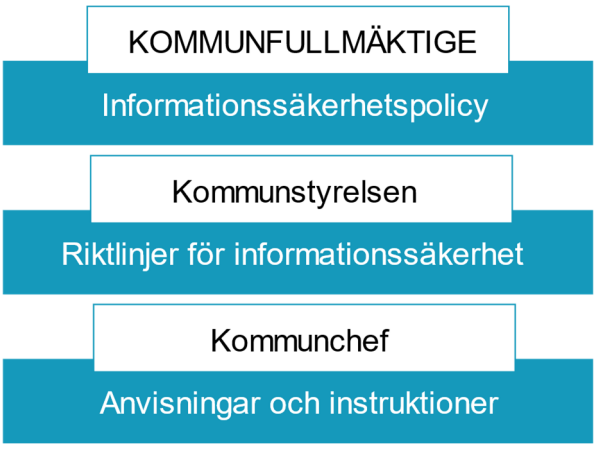
Föreliggande Informationssäkerhetspolicy utgör tillsammans med Riktlinjer för informationssäkerhet grunden för Lilla Edets kommuns arbete med informationssäkerheten inom sina verksamhetsområden.

Informationssäkerhetspolicy

Informationssäkerhet är den del i kommunens ledningsprocess som avser hantering av verksamhetens information och en viktig del för att följa Lag (2018:1174). Policyn beskriver kommunens mål och inriktning för informationssäkerhetsarbetet. Informationssäkerhetspolicyn och riktlinjer styr kommunens informationssäkerhetsarbete.

Policyns roll i informationssäkerhetsarbetet

Informationssäkerhetspolicyn redovisar ledningens mål för informationssäkerhetsarbetet och viljeinriktning att följa Lag (2018:1174). Policyn konkretiseras i riktlinjer för informationssäkerhet. Informationssäkerhetspolicyn beslutas av kommunfullmäktige. Informationssäkerhetsriktlinjerna beslutas av kommunstyrelsen.



Allmänt om informationssäkerhet

Information är en av kommunens viktigaste tillgångar och hanteringen av den är en viktig del i kommunens arbete.

Utgångspunkter i kommunens arbete med informationssäkerhet är framförallt:

- Lagar, förordningar och föreskrifter
- Kommunens egna krav
- Avtal

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer. Informationssäkerheten omfattar kommunens informationstillgångar utan undantag.

Informationssäkerhet innebär att säkerställa informationens:

- **RIKTIGHET** - att information inte kan förändras vare sig av obehöriga, av misstag eller på grund av funktionsstörning. Informationen ska vara tillförlitlig, korrekt och fullständig.

- **SEKRETESS** - att innehållet i dokument, information och handlingar inte görs tillgängliga eller avslöjas för obehörig.

- **SPÅRBARHET** - att i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt, användare, skrivare, dator eller system/program. Det ska gå att se vem som tagit del av informationen, vilka förändringar som har skett och av vem dessa har utförts.

- **TILLGÄNGLIGHET** - att information och informationstillgångar kan utnyttjas efter behov, i förväntad utsträckning och inom önskad tid utifrån de krav som ställs på verksamheten.

Informationssäkerhet är en integrerad del av kommunens verksamhet. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till informationssäkerhetsarbetet.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för kommunens informationstillgångar.

Alla verksamheter inom kommunen omfattas av denna informationssäkerhetspolicy vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna.

Den som använder kommunens informationstillgångar på ett sätt som strider mot denna policy och tillhörande riktlinjer kan bli föremål för disciplinära, alternativt rättsliga, åtgärder.

Mål för kommunens informationssäkerhetsarbete

Kommunens mål med informationssäkerhetsarbetet är att:

- Personal har kunskap om gällande informationssäkerhetsregler.
- Informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man.
- Lagar, förordningar och föreskrifter är kända och följs.
- Ingångna avtal är kända och följs.
- Krishanteringsförmågan upprätthålls.
- Alla investeringar både i form av information samt teknisk utrustning har skydd i tillräcklig grad.
- Det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation.
- Hotbilden för varje enskilt informationssystem som är av vikt för verksamheten analyseras fortlöpande.
- Händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs.
- Årliga mål för verksamheten ska ingå i den normala verksamhetsplaneringen.

Roller och ansvar

Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhet.

Kommunchefen har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den av kommunstyrelsen fastställda informationssäkerhetspolicyn.

Kommunchefen fastställer, på delegation av kommunstyrelsen, kommunövergripande riktlinjer och instruktioner.

Kommunchefen ansvarar för att systemägare utses för respektive informationssystem.

Systemägaren är ansvarig för säkerheten i sitt system.

IT-chefen ansvarar för att tillse att driftsäkerheten överensstämmer med systemägarens anvisningar

IT-chefen har det operativa ansvaret för samordning av informationssäkerhetsarbetet.

Revidering och uppföljning

Uppföljning är en viktig del av informationssäkerhetsarbetet. Uppföljningen ska bevaka:

- Att beslutade åtgärder är genomförda
- Att mål är uppfyllda.
- Att riktlinjer följs.

Policy och riktlinjer ska löpande följas upp och revideras vid behov.