Policy för informationssäkerhet

Beslutande instans: Kommunfullmäktige
Beslutsdatum och -paragraf (inkl. revideringar): 2023-02-27 §14
Dokumentansvarig enhet: Enheten för juridik och informationssäkerhet

Innehållsförteckning

1. Inledning

Information är en grundläggande byggsten i en organisation, på samma sätt som medarbetare, lokaler och utrustning. Det är en av kommunens viktigaste tillgångar och behöver som sådan skyddas genom ett systematiskt informationssäkerhetsarbete. På så sätt kan Skara kommun öka kvaliteten i och förtroendet för vår verksamhet.

Arbete med informationssäkerhet innefattar flera delar. Utöver införande av administrativa regelverk såsom policys och riktlinjer handlar det även om införande av tekniskt skydd i form av bland annat brandväggar och kryptering samt införande av fysiskt skydd som till exempel skal- och brandskydd. Informationssäkerhetsarbete handlar om att ta ett helhetsgrepp och skapa ett fungerande långsiktigt arbetssätt för att ge organisationens information det skydd den behöver.

Informationssäkerhet bygger på tre grundprinciper:

Konfidentialitet	att information endast finns tillgänglig för behöriga.
Riktighet	att information är korrekt, aktuell, fullständig och inte kan ändras av obehöriga.
Tillgänglighet	att information finns tillgänglig för behöriga när den behövs.

Regeringen har genom en nationell strategi[1] fastslagit att informationssäkerheten på kommunal nivå är i behov av att utvecklas. En av målsättningarna i strategin är att statliga myndigheter, kommuner och regioner ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett strukturerat och riskbaserat informationssäkerhetsarbete. Därigenom ska man kunna säkerställa den fortsatta digitaliseringen av samhället, samtidigt som man hävdar Sveriges säkerhet och nationella intressen, såsom mänskliga fri- och rättigheter och samhällets funktionalitet.

[1] Nationell strategi för samhällets informations- och cybersäkerhet (Skr. 2016/17:213)

2. Lagstiftning

På informationssäkerhetsområdet finns det ett flertal lagar som på övergripande nivå ställer krav på kommunen och dess verksamheter.

- **Dataskyddsförordningen (GDPR, 2016/679):** ställer krav på hanteringen av personuppgifter.

- **Säkerhetsskyddslagen (2018:585):** ställer krav på verksamheter som är väsentliga för Sveriges säkerhet.

- **NIS-direktivet (lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster):** ställer krav på vissa verksamheter i syfte att uppnå en hög nivå på säkerheten i nätverk och informationssystem. En kommun kan uppfylla kriterierna för att bedriva samhällsviktig tjänst inom sektorerna energi, hälso- och sjukvård samt leverans och distribution av dricksvatten.

Därutöver finns även verksamhetsspecifika krav på informationssäkerhet i ibland annat skollagen, socialtjänstlagen och hälso- och sjukvårdslagen, i form av tystnadsplikt och sekretess.

3. Intressenter

De myndigheter som stödjer och följer upp informationssäkerhetsarbetet är bland andra:

- Myndigheten för samhällsskydd och beredskap (MSB)
- Sveriges kommuner och regioner (SKR)
- Integritetsskyddsmyndigheten (IMY)

NIS-direktivet följs dessutom upp av Statens energimyndighet, Livsmedelsverket och Inspektionen för vård och omsorg (IVO). Säkerhetsskyddslagen följs upp av Säkerhetspolisen.

4. Informationssäkerhetspolicyns omfattning

Denna informationssäkerhetspolicy utgör kommunens viljeinriktning för att hantera kommunens information på ett systematiskt och informationssäkert sätt.

Kommunens informationssäkerhetpolicy omfattar all information som kommunens verksamheter äger och hanterar. Arbetet med informationssäkerhet ska säkerställa att kommunens informationstillgångar skyddas utifrån sitt skyddsvärde, oavsett om de hanteras manuellt eller digitalt.

5. Strategiska målsättningar

I sitt arbete med informationssäkerhet ska kommunen utgå från ett antal strategiska målsättningar.

5.1. Kommunen ska bedriva ett systematiskt informationssäkerhetsarbete

Kommunen ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarden SS-ISO/IEC 27000-serien (ISO 27000-serien). Detta ska utgöra kommunens ledningssystem för informationssäkerhet.

Kommunen ska utforma informationssäkerhetsarbetet så att det möter de lagkrav som berör kommunen.

Kommunen ska upprätta följande styrdokument, som krävs för att ett systematiskt informationssäkerhetsarbete ska kunna bedrivas:

- Riktlinje för organisation och roller
- Riktlinje för medarbetare och förtroendevalda
- Riktlinje för fysisk och teknisk säkerhet
- Riktlinje för informationssäkerhet vid upphandlingar
- Rutin för avvikelse- och incidentrapportering
- Rutin för internkontroll

I den mån det är nödvändigt ska även ytterligare styrdokument upprättas.

5.2. Kommunen ska ha en informationssäkerhetsorganisation

Kommunen ska upprätta en organisation med tydliga roller och ansvarsfördelningar för genomförandet av det systematiska informationssäkerhetsarbetet.

Det ska finnas en riktlinje som beskriver organisationen för informationssäkerhet och de roller som ingår.

5.3. Chefer, medarbetare och förtroendevalda ska ha en grundläggande kompetens inom informationssäkerhet

Kommunen ska säkerställa att samtliga chefer, medarbetare och förtroendevalda erbjuds relevant utbildning inom informationssäkerhet. Utbildning ska samordnas av informationssäkerhetssamordnaren. Chefer har ett ansvar att se till att deras

medarbetare har rätt förutsättningar för att hantera de informationstillgångar deras arbete kräver.

Det ska finnas en riktlinje för informationssäkerhet för medarbetare och förtroendevalda.

5.4. Kommunen ska fastställa krav på fysisk och teknisk säkerhet

Kommunen ska fastställa informationssäkerhetsrelaterade krav på den fysiska och tekniska säkerheten i samtliga system som används i verksamheten.

Det ska finnas en riktlinje som beskriver fysisk och teknisk säkerhet.

5.5. Kommunen ska fastställa krav vid upphandling och i leverantörsavtal

Kommunen ska fastställa de informationssäkerhetsrelaterade krav som ska ställas vid upphandlingar och i avtal med leverantörer som kommer hantera information inom verksamheten.

Kommunen ska kontrollera att leverantörerna följer de krav som ställs.

Det ska finnas en riktlinje för informationssäkerhet vid upphandlingar.

5.6. Kommunen ska ha ett system för uppföljning vid brister och incidenter

Kommunen ska ha ett system för när, var och hur incidenter och avvikelser ska rapporteras till berörda myndigheter i enlighet med gällande lagkrav. Det ska finnas en rutin för avvikelse- och incidentrapportering.

5.7. Kommunen ska följa upp sitt informationssäkerhetsarbete

Kommunen ska följa upp efterlevnaden av sitt informationssäkerhetsarbete via internkontroll. Det ska finnas en rutin för internkontroll.