Riktlinjer för informationssäkerhet

Organisation och roller

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

Innehållsförteckning

Termer och definitioner

Term	Definition
Data	Representation av fakta i form av t.ex. tecken eller signaler som är lämpad för överföring, tolkning eller bearbetning av människor eller automatiska hjälpmedel.
CISO	Förkortning av Chief Information Security Officer. På svenska ofta benämnd som informationssäkerhetssamordnare eller informationssäkerhetsstrateg.
Information	Innebörd av data, dvs. data tolkad av människor.
Informationssäkerhet	Konfidentialitet, riktighet och tillgänglighet hos information.
Informationssäkerhetspolicy	Kommunens viljeinriktning med informationssäkerhet, uttryckt av dess ledning.
Informationstillgångar	Information som är av värde för organisationen. Avser även de resurser som hanterar den, exempelvis människor, papper, mjukvara, hårdvara och immateriella tillgångar (t.ex. rykte).
Informationsägare	Den som äger och ansvarar för att information är riktig och tillförlitlig samt för det sätt på vilket informationen sprids. Informationsägaren är därmed riskägare för den information som ska hanteras i ett IT-system eller en lösning.
Klassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss informationstillgång.

Personuppgiftsansvarig	Den som vid behandling av personuppgifter bestämmer för vilka ändamål personuppgifterna ska behandlas och hur behandlingen ska gå till.
Riskägare	Person som tar ansvar för varje risk.
Systematiskt informationssäkerhetsarbete	Att arbeta förebyggande och att kontinuerligt anpassa skyddet för information utifrån organisationens behov och risker. Då finns informationen tillgänglig när vi behöver den, vi kan lita på att den är riktig och inte manipulerad och att endast behöriga personer får ta del av den.
Verksamhetsanalys	Genomförs för att identifiera och klassificera verksamhetens informationstillgångar. De arbetsuppgifter som genomförs under en verksamhetsanalys är: • identifiera informationstillgångarna • identifiera kraven (interna och externa) • klassificera informationstillgångar

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 med 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.

2. Ansvar

2.1. Grundprincip

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret och sträcker sig på så sätt från den politiska ledningen, genom tjänstemannaledningen och ner till varje enskild medarbetare. Den som är ansvarig för en viss verksamhet (avdelning, enhet, process, projekt osv.) är också formellt ansvarig för informationssäkerheten i verksamheten.

2.2. Ledning och ansvar

Kommunfullmäktige fastställer policy och riktlinjer för informationssäkerhet och uttrycker därigenom viljeinriktningen för kommunens arbete med informationssäkerhet.

Kommunstyrelsen verkställer kommunfullmäktiges beslut och har övergripande ansvar för informationssäkerhetsarbetet. Kommunstyrelsen är personuppgiftsansvarig och utser dataskyddsombud för sina verksamheter.

Nämnderna i kommunen är ytterst ansvariga för att informationssäkerheten håller rätt och relevant nivå i deras respektive verksamheter. Nämnderna är personuppgiftsansvariga för sina verksamheter och utser dataskyddsombud.

Kommunala bolag har ansvar för informationssäkerheten i sina egna verksamheter. Detta kan också regleras närmare i särskilda ägardirektiv. Kommunala bolag är personuppgiftsansvariga för sina verksamheter och utser dataskyddsombud.

Chefer har ansvar för informationssäkerhetsarbetet i sina verksamheter. Chefer ansvarar för att medarbetarna har rätt behörighet, kompetens och förutsättningar för att på ett säkert sätt kunna hantera den information de har tillgång till.

Informationsägare är den som äger en viss information och ansvarar för dess informationssäkerhet – dvs. ansvarar för att den är riktig och tillförlitlig, samt för det sätt på vilket informationen sprids. Eftersom ansvaret för informationssäkerhet ska följa det ordinarie verksamhetsansvaret är det oftast chefen för en förvaltning, avdelning eller enhet som är informationsägare.

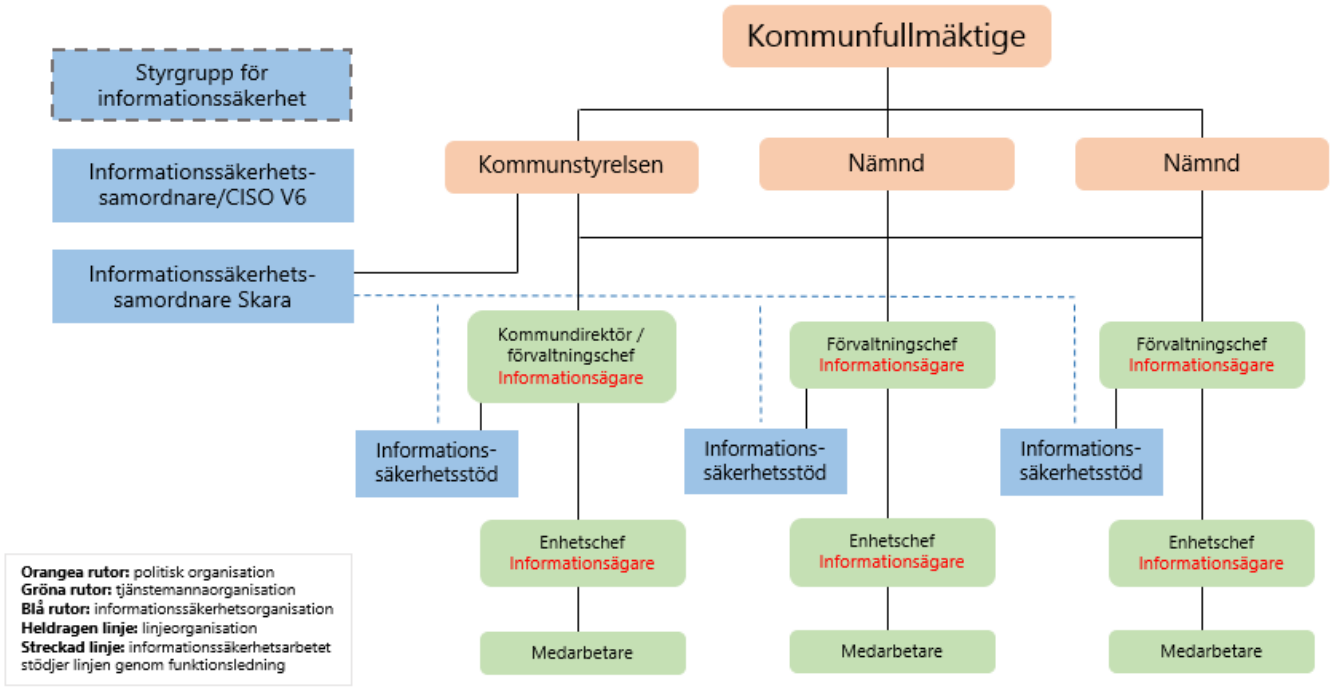
Informationsägaren har ansvar för att säkerställa att informationsbärare (såsom exempelvis IT-system, medarbetare, pärmar och dokumentskåp) har rätt och relevant tekniskt och fysiskt skydd för den information de innehåller.

Informationsägaren är därutöver ansvarig för att hantera risker och ställa krav på informationssäkerhet med hjälp av till exempel verksamhetsanalyser, där informationstillgångarna identifieras och klassificeras. Om en informationsbärare används gemensamt av flera informationsägare bör sådana åtgärder samordnas.

Medarbetare och förtroendevalda hanterar kommunens informationstillgångar och har ett ansvar att följa kommunens informationssäkerhetspolicy och underliggande styrdokument för informationssäkerhet. De har också ansvar för att uppmärksamma fel och brister i informationshantering, utrustning och informationsinnehåll samt för att rapportera sådana i enlighet med fastställda rutiner.

3. Organisation

Bilden nedan visar hur organisationen för informationssäkerhet ser ut i Skara kommun.



4. Roller

4.1. Informationssäkerhetssamordnare V6

V6-kommunerna har en gemensam funktion i form av informationssäkerhetssamordnare/CISO. Funktionen är placerad på Göliska IT.

4.2. Informationssäkerhetssamordnare Skara

Informationssäkerhetssamordnare i Skara arbetar strategiskt med att få kommunens informationssäkerhetsarbete att fungera. Den har ansvar för att ge strategiskt stöd till ledning, verksamhetschefer och medarbetare, så att de i sin tur kan ta ansvar för informationssäkerheten i sin verksamhet.

Informationssäkerhetssamordnaren har ansvar för att ta fram och underhålla styrdokument, samordna träffar mellan informationssäkerhetsstöden på förvaltningarna och utgöra ett strategiskt stöd för dem.

4.3. Informationssäkerhetsstöd förvaltning

Informationssäkerhetsstöd på kommunens förvaltningar arbetar i huvudsak operativt genom att hantera informationssäkerhetsarbetet inom den egna förvaltningen. Arbetet utförs på uppdrag av informationsägaren och i dialog med informationssäkerhetssamordnare.

Hur mycket tid rollen som informationssäkerhetsstöd tar varierar beroende på den aktuella förvaltningens storlek och behov. Rollen bör dock som minst utgöra 20 % av medarbetarens arbetstid.

5. Samverkan

5.1. Styrgrupp för informationssäkerhet

Styrgruppen för informationssäkerhet är en kommunövergripande grupp som leds av informationssäkerhetssamordnare Skara. Som utgångspunkt ingår kanslichef, GDPR-samordnare, säkerhetssamordnare, digitaliseringschef och arkivarie i gruppen. Vid behov ska även andra kompetenser bjudas in. Sammanträder löpande.

5.2. Informationssäkerhetssamordnare V6

Informationssäkerhetssamordnarna i V6-kommunerna träffas regelbundet under ledning av informationssäkerhetssamordnare V6/CISO.

5.3. Informationssäkerhetsstöd inom kommunen

Informationssäkerhetsstöden i kommunens förvaltningar träffas regelbundet under ledning av kommunens informationssäkerhetssamordnare.