ÖSTERSUNDS KOMMUN

Program
Strategi
➢ Policy
Riktlinje

Informationssäkerhetspolicy Östersunds kommun

Dokumentnamn:	Fastställd av:	Gäller från:
Informationssäkerhetspolicy	Kommunfullmäktige 2019-05-28, § 95, dnr: 01891/2018	2019-05-28
Berörd verksamhet:	Dokumentansvarig:	
Alla nämnder och förvaltningar	Informationssäkerhetsstrateg	

1 Inledning och syfte

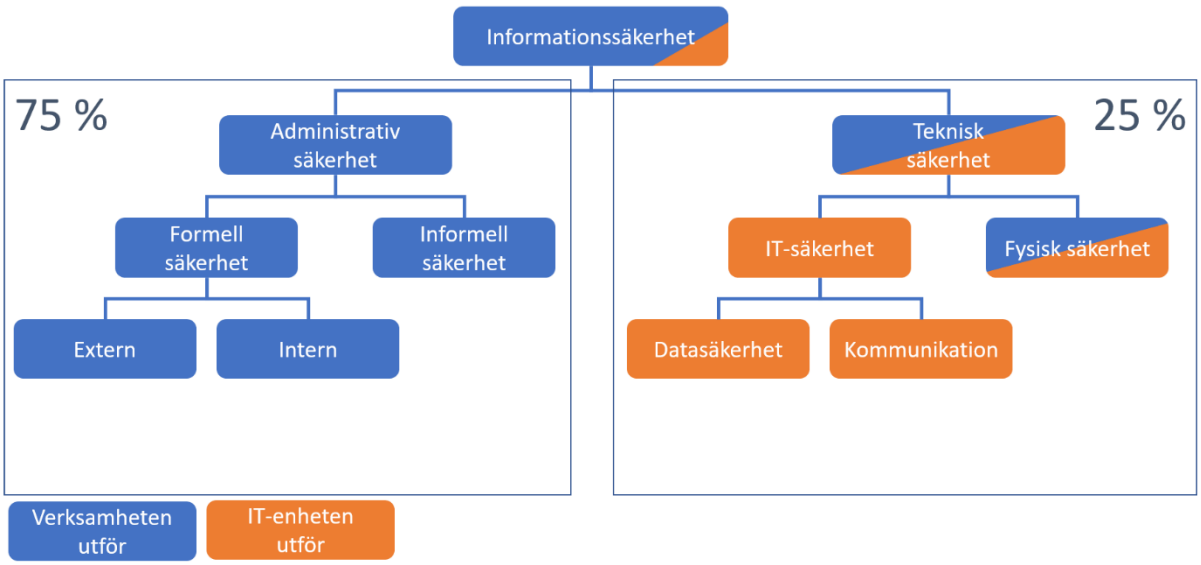
Kommunens informationssäkerhetsarbete ska syfta till att kommunens information vid varje given tidpunkt ska ha ett lämpligt skydd, oavsett om informationen är muntlig, pappersbunden eller digital. Skyddet ska utgå ifrån genomförd informationssäkerhetsklassificering och därmed vara tillgänglig för de som behöver den och har behörighet att ta del av informationen. Informationen ska också vara komplett och korrekt, samt ha en lämplig nivå av spårbarhet. Informationssäkerhetsarbetet måste ständigt anpassas efter aktuella hotbilder, både vad avser yttre såväl som inre hot. Det kan handla om t.ex. kunskapsbrister hos medarbetare eller intrång både i fysiska miljöer men också i kommunens IT-miljö.

Syftet med denna policy är att tydliggöra vilket förhållningssätt som gäller för att säkerställa informationssäkerhet inom hela den kommunala verksamheten, detta innefattar ej de kommunala bolagen eller kommunförbunden.

1.1 Vad är 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.



Figur 1 Karta över informationssäkerhetsarbetets olika delar

Arbetet med informationssäkerhet består av både administrativa och tekniska säkerhetsåtgärder. Som illustreras i figur 1 är merparten av arbetet kopplat till de administrativa åtgärderna. Det är respektive verksamhet som ansvarar för de administrativa åtgärderna, både beslut om och genomförande av, medan IT-enheten bistår med stöd vad gäller beslut om delar av de tekniska säkerhetsåtgärderna, och i vissa fall även genomföra av dessa åtgärder.

Målet med informationssäkerhetsarbetet är att Östersunds kommun ska ha en effektiv informationsförsörjning som skapar förutsättningar för ett effektivt arbete i kommunen samt bygger förtroende hos bland annat medborgare och medarbetare.

2 Östersunds kommuns förhållningssätt för informationssäkerhet

Det är Östersunds kommuns förhållningssätt för informationssäkerhet att:

- Informationssäkerhetsarbetet ska bedrivas systematiskt genom ett ledningssystem för informationssäkerhet enligt standarderna ISO/IEC 27001 och ISO 27002.
- All information som hanteras i kommunen ska skyddas på en lämplig nivå, utifrån genomförda informationssäkerhetsklassificeringar, riskanalyser och organisationens riskacceptans.
- Det ska finnas tydliga regler för hur information ska hanteras inom Östersunds kommun, det är särskilt viktigt i de fall Östersunds kommun hanterar integritetskänslig information. All hantering av information inom Östersunds kommun ska ske i enlighet med kommunens interna regler, gällande rätt samt följa överenskommelser i ingångna avtal.
- All personal ska ha tillräckliga kunskaper om kommunens informationssäkerhetsarbete, förväntas känna till gällande regler och ta ansvar för sin del i informationssäkerhetsarbetet.

3 Roller och ansvar inom informationssäkerhet

3.1 Kommunfullmäktige

Kommunfullmäktige beslutar om vilken informationssäkerhetspolicy som ska gälla för kommunen och har det yttersta ansvaret för kommunens informationssäkerhetsarbete.

3.2 Kommunstyrelsen, övriga nämnder och Kommunrevisionen

Kommunstyrelsen ansvarar för att samordna, utveckla och leda arbetet med informationssäkerhet inom hela den kommunala verksamheten. Kommunstyrelsen fastställer riktlinjer för informationssäkerhetsarbetet.

Övriga nämnder och Kommunrevisionen ansvarar för att efterleva riktlinjer och övriga beslut som fastställs av Kommunstyrelsen gällande informationssäkerhet.

3.3 Kommundirektören

Kommundirektören har det yttersta operativa ansvaret för kommunens informationssäkerhetsarbete, att lämpliga roller finns på plats inom organisationen och att informationssäkerhetsstrateg samt övrig personal har den kunskap och de resurser som krävs för att säkerställa att kommunens mål kring informationssäkerhet nås.

3.4 Förvaltningschef

Varje förvaltningschef är ansvarig för informationssäkerheten inom sin förvaltning. Varje förvaltningschef måste därför upprätta de förvaltningsspecifika rutiner som behövs för att säkerställa att denna policy, inklusive tillhörande riktlinjer, är lämpliga, väl kända och följs inom den egna verksamheten.

3.5 Informationssäkerhetsstrateg

Kommunens informationssäkerhetsstrateg ska arbeta samordnande för det kommunövergripande informationssäkerhetsarbetet. Informationssäkerhetsstrategen ansvarar för att stödja ansvariga funktioner i arbetet med att identifiera, ta fram och uppdatera kommunövergripande styrande dokument för informationssäkerhetsarbetet. Vidare ansvarar informationssäkerhetsstrategen för att följa upp det kommunövergripande informationssäkerhetsarbetet samt för att skapa underlag för beslut om hur arbetet ska vidareutvecklas

3.6 Informationsägare

För all information ska det finnas en informationsägare. Informationsägaren ansvarar för informationsinnehållet samt informationssäkerheten. Informationsägare kan till exempel vara systemägare eller processägare.

3.7 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. Det är varje chefs ansvar att säkerställa att de egna medarbetarna har tillräcklig kunskap om denna policy, tillhörande riktlinjer och andra styrande dokument på området.

4 Uppföljning och revidering

Kommunens informationssäkerhetsstrateg ansvarar för att uppföljning och revidering av denna policy sker minst en gång vartannat år. I samband med revidering ska samtliga relaterade styrdokument gås igenom och vid behov uppdateras.