



Riktlinjer för informationssäkerhet

Beslutsdatum	<i>[Beslutsdatum]</i>
Diarienummer	<i>[Diarienummer]</i>
Reviderat	-
Lagstadgat styrdokument	-
Ersätter styrdokument	Policy och riktlinjer för informationssäkerhet
Uppföljning	Vart fjärde år
Ansvar	Kommunstyrelsen

Inledning

Information är en av kommunens mest strategiska resurser och alla verksamheter är beroende av tillförlitlig information. Vi klarar idag i princip ingen verksamhet utan tillgång till våra informationsresurser och störningar i våra mest kritiska system kan leda till allvarliga kriser och drabba enskilda och deras hälsa, innebära försenade utbetalningar och påverka förtroendet för förvaltning och service.

Information kan förekomma i många olika former. Oftast är den lagrad elektroniskt men information kan också finnas tryckt eller enbart nedskrivet och yttras i en konversation. Oavsett form så omfattas denna policy av samtliga informationstillgångar oberoende om den behandlas manuellt eller med informationsteknologi.

Informationssäkerhet är en del i kommunens lednings- och kvalitetsarbete och är en viktig del för att nå målen om en effektiv administration och förvaltning. Kommunen tar ansvar för sina informationstillgångar genom att arbeta strukturerat med informationssäkerhet i den egna verksamheten och ställa krav på upphandlade leverantörer. Denna policy tydliggör kommunens övergripande principer och förhållningssätt för arbetet med informationssäkerhet. I policy för IT-säkerhet regleras säkerhet i IT-system, med detta avses data- och informationssystem, datanät, datorer och övrig datautrustning.

Vägledande principer

Informationssäkerhet definieras som

- Konfidentialitet: Att information inte tillgängliggörs eller avslöjas till obehörig.
- Riktighet: Att informationen är korrekt, aktuell och fullständig.
- Tillgänglighet: Att informationen är åtkomlig och användbar av behörig.

För kommunens informationssäkerhetsarbete ska följande gälla:

- Arbetet ska bygga på en helhetssyn och omfatta processer, människor och teknik.



Beslutsdatum: [Beslutsdatum]	Diarienummer: [Diarienummer]
Dokumentnamn: Riktlinjer informationssäkerhet	

- Att personal har tillräckliga kunskaper om informationssäkerhet i förhållande till sina arbetsuppgifter.
- Det är säkerställt att det finns en förmåga att upprätthålla en säker informationshantering som är effektiv och bidrar till ökat skydd och stöd för medarbetare, tredje man och samarbetspartners.
- Vara förebyggande och proaktiv och kännetecknas av en god förmåga och organisation för att kunna hantera incidenter, allvarliga störningar och kriser.
- Ta tillvara möjligheterna i aktiv samverkan med det omgivande samhället, inbegripande myndigheter, företag och nätverk som kan vara ett stöd.
- Informationssäkerhetsarbetet ska ta sin utgångspunkt i standarden ISO/IEC 27000, Dataskyddsförordningen och övrigt gällande lagar och förordningar.
- Policyn konkretiseras med beslut om, tillämpningsrutiner och övriga systemnära beslut.
- Varje nämnd är personuppgiftsansvarig och samtliga informationstillgångar ska vara förtecknade inom respektive nämnd.
- Det sker kontinuerlig uppföljning av system och rutiner.

Organisation och ansvar

Kommunfullmäktige fastställer riktlinjer för informationssäkerhet..

Kommundirektören får i uppdrag att besluta om tillämpningsrutiner och säkerställa att arbetet bedrivs på ett effektivt sätt.

Personuppgiftsansvariga är samtliga nämnder i kommunen.

Inom kommunen utnämns ett Dataskyddsombud för samtliga nämnder. Ansvar för informationssäkerhet följer verksamhetsansvaret med särskilt ansvar på chefsnivå.

IT-chefen ansvarar för att säkerheten i kommunens IT-miljö som tjänster, processer, system infrastruktur etc. är tillräcklig och uppfyller verksamhetens krav, legala krav och beslutad policy, riktlinje och rutiner.

Säkerhetschefen samordnar det övergripande och strategiska arbetet för att leda och utveckla informationssäkerhetsarbetet

Varje anställd ansvarar för att gällande regler för informationssäkerheten följs samt att upptäckta brister rapporteras enligt fastställda rutiner.

Uppföljning

Informationssäkerhetsarbetet ska kontinuerligt följas upp och utvärderas enligt beslutade rutiner. Denna riktlinje ska följas upp i samband med den återkommande övergripande risk- och sårbarhetsanalysen. I övrigt tar kommunstyrelsen initiativ till revidering av riktlinjen.