# Informationssäkerhetspolicy

Diarienummer: KS 2022-00396 1.3.1

Antagen: Kommunfullmäktige, 2023-12-09, § 142

Reviderad:

Dokumentansvarig förvaltning: Kommunstyrelsens förvaltning

Dokumentet gäller för: Söderköpings kommun

Dokumentet gäller till och med: Tillsvidare

**Postadress**
Söderköpings kommun
614 80 Söderköping

**Besöksadress**
Kommunhuset
Storängsallén 20

**Kontakt**
0121-181 00
kommun@soderkoping.se

**Org.nr och webbplats**
212000-0464
www.soderkoping.se

# Innehållsförteckning

## Inledning

Denna policy gäller för informationssäkerhet inom Söderköpings kommun och kommunala bolag. I de fall extern part hanterar Söderköpings kommuns eller kommunala bolags information ska denne genom avtal eller liknande förbindas att följa motsvarande krav på hantering av information som gäller för kommun och bolag.

Informationssäkerhetspolicyn redovisar Söderköpings kommuns och kommunala bolags övergripande mål och inriktning med informationssäkerhet samt hur ansvaret är fördelat. Styrdokumentet riktlinjer för informationssäkerhet är mer detaljerat och konkretiserar denna informationssäkerhetspolicy. Kommunala bolag behöver ha egna riktlinjer för informationssäkerhet som konkretiserar policyn. Bolag rekommenderas att i sitt arbete utgå från Söderköpings kommuns styrande och stödjande dokument inom området.

## Om informationssäkerhet

Information finns i alla kommunens verksamheter och bolag. Informationen rör exempelvis vår personal, våra tjänster, vår ekonomi och vår omgivning med medborgare, företag och civila samhället. Information är därför en av kommunens viktigaste tillgångar.

Information är medieoberoende och kan till exempel vara text, ljud, bilder, film och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal.

Informationssäkerhet handlar om hur vi skyddar information utifrån legala krav och för att möta interna och externa intressenters behov. Kraven ställs utifrån fyra aspekter:

- konfidentialitet - att informationen inte tillgängliggörs eller avslöjas till obehörig,
- riktighet - att informationen är korrekt, aktuell, fullständig,
- tillgänglighet - att informationen är åtkomlig och användbar av behörig,
- spårbarhet - att förändring i information går att spåra och återskapa.

## Mål med informationssäkerhetsarbetet

Informationssäkerhet har inget egenvärde utan ska bidra till att Söderköpings kommun och kommunala bolag når sina övergripande visioner, strategier och mål.

Söderköpings kommun och kommunala bolag ska uppnå och upprätthålla en informationshantering som:

- är robust, säker och tillförlitlig,
- möjliggör ett aktivt medverkande i det digitala samhället,
- bidrar till att uppsatta mål nås gällande exempelvis kvalitet, effektivitet och personlig integritet,
- motsvarar interna och externa intressenters behov och förväntningar,
- efterlever krav i lagar, förordningar, föreskrifter och avtal,
- förebygger, hanterar och rapporterar incidenter,
- bygger på en rättvis och lärande kultur,
- stärker medarbetarnas säkerhetsmedvetande och förmåga att upprätthålla informationssäkerhet i vardagen,
- värnar om den personliga integriteten med hänsyn till den enskildes friheter och rättigheter.

## Principer och arbetssätt

Söderköpings kommun och kommunala bolag ska arbeta med informationssäkerhet på ett sätt så att ovanstående mål uppfylls.

Arbetet med informationssäkerhet ska:

- vara systematiskt och bygga på den etablerade standardserien SS-ISO/IEC 27000,
- utgå från Söderköpings kommuns ledningssystem för informationssäkerhet (LIS) som är normerande, stödjande och kontrollerande,
- löpande ses över och förbättras, eftersom Söderköpings kommun och dess omvärld, inklusive hotbild, är under ständig förändring,
- vara proaktivt, men också ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa,
- hantera avvikelser och undantag på ett strukturerat och ordnat sätt,
- bygga på Söderköpings kommuns värderingar och uppfylla lämpliga krav relaterade till informationens skyddsbehov, systemens skyddsbehov, verksamhetens behov, externa krav samt rådande hotbild,
- vara väl kommunicerat till verksamheten; chefer ska tillse att all personal fortlöpande får information och utbildning för att nå och upprätthålla ett högt säkerhetsmedvetande och för att kunna leva upp till denna policy och underliggande riktlinjer för informationssäkerhet,
- följa och samverka med omgivande samhället såsom myndigheter, företag och nätverk - särskilt normgivande aktörer inom informationssäkerhet såsom Sveriges kommuner och regioner (SKR), Myndigheten för samhällsskydd och beredskap (MSB) och Swedish Standards Institute (SIS),
- i tillämpliga delar samordnas med kommunens arbete rörande säkerhet och dataskydd.

## Roller och ansvar

Ansvaret för informationssäkerhet följer ordinarie verksamhetsansvar. Detta gäller från kommunledning till enskild medarbetare och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för att, utifrån informationsägarens krav, skydda den information som hanteras inom verksamheten.

Alla anställda i Söderköpings kommun och bolag har ett ansvar för att upprätthålla informationssäkerheten och uppmärksamma brister.

Kommunala bolag ska bedriva ett systematiskt informationssäkerhetsarbete enligt Söderköpings kommuns gällande policy. Kommunala bolag behöver ha egna riktlinjer för informationssäkerhet som konkretiserar policyn. Bolag rekommenderas att i sitt arbete utgå från Söderköpings kommuns styrande och stödjande dokument inom området.

Söderköpings kommun samt kommunala bolag behöver var för sig ha en funktion som har till uppgift att leda, samordna och följa upp informationssäkerhetsarbetet inom respektive organisation (normalt förkortad CISO[1]).

[1] Enligt Myndigheten för samhällsskydd och beredskap (MSB) är det lämpligt att använda den engelska förkortningen CISO (Chief Information Security Officer).

Varje förvaltning inom Söderköpings kommun ska utse kontaktpersoner som driver och samordnar verksamhetens informationssäkerhetsarbete. Kommunala bolag bedömer själva hur de hanterar dessa roller.

Kommunens informationssäkerhets- och dataskyddssamordnare (CISO) och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor fungerar som stöd till kommunens verksamheter att fullfölja informationssäkerhets-ansvaret.

Nedan beskrivs informationssäkerhetsansvar för ett antal centrala roller och funktioner. Dessa roller och ytterligare roller beskrivs utförligare i riktlinjer för informationssäkerhet.

**Informationsägare** - det yttersta övergripande ägarskapet för informationssäkerheten ligger hos den politiska ledningen i form av Kommunfullmäktige, Kommunstyrelse, nämnder och kommunala bolags styrelser. De är informationsägare inom sina respektive områden och ska därmed arbeta systematiskt för att säkerställa att informationen skyddas enligt gällande författningar, policy och riktlinjer.

**Kommunfullmäktige** - fastställer den informationssäkerhetspolicy som ska gälla för kommun och bolag.

**Kommunstyrelsen** - har det yttersta ansvaret för kommunens informationssäkerhet och ska följa upp efterlevnaden av kommunens informationssäkerhetspolicy. Kommunstyrelsen ansvarar för samordningen av informationssäkerhetsarbetet i kommunen. Kommunstyrelsen ansvarar för att kommunövergripande riktlinjer för informationssäkerhet fastställs och hålls aktuella.

**Nämnder** - är ytterst ansvarig för informationssäkerhet inom sitt verksamhetsområde och ska säkerställa att verksamheten följer antagna riktlinjer och rutiner.

**Säkerhetschef** - har det övergripande ansvaret att leda, utveckla och samordna Söderköpings kommun säkerhetsarbete.

**Informationssäkerhets- och dataskyddssamordnare (CISO)** - har det övergripande ansvaret att leda, utveckla, samordna och följa upp informationssäkerhetsarbetet. Ska arbeta i samråd med säkerhetschef och IT- och digitaliseringschef.

**IT-säkerhetssamordnare** - samordnar arbetet med IT-säkerhet i Söderköpings kommuns IT-miljö.

**Objektägare** - har det övergripande ansvaret för informationssäkerheten i objektet. Objektägaren ska, utifrån informationsägarens krav, skydda den information som hanteras inom objektet samt säkerställa att arbetet med att skydda informationen bedrivs enligt gällande författningar, policy och riktlinjer.

**Objektägare IT** - har det övergripande ansvaret för att IT-säkerheten i objektet uppfyller verksamhetens krav samt gällande författningar, policy och riktlinjer.

**Objektförvaltare** - har det funktionella och dagliga ansvaret för system. Objektförvaltare fungerar i hög grad som objektägarens utförare och ser till systemets funktionalitet samt planerade/beslutade aktiviteter genomförs och upprätthålls.

**Teknisk objektförvaltare** - har det IT-tekniska ansvaret för verksamhetssystem. Teknisk objektförvaltare fungerar som objektägare IT:s utförare och ser till att systemets funktionalitet utifrån IT-drift och IT-säkerhet upprätthålls enligt kommunens förvaltningsmodell.

**Medarbetare** - alla medarbetare har ett ansvar för verksamhetens informationssäkerhet. Varje anställd ska i eget arbete följa riktlinjer för informationssäkerhet samt eventuella verksamhetsspecifika regler.

**Dataskyddsombud** - ansvarar för att informera och ge råd till personuppgiftsansvariga nämnder och bolag kring vilka skyldigheter som gäller enligt dataskyddsförordningen. Dataskyddsombudet ska också bevaka att reglerna följs och fungera som kontaktperson för Integritetsskyddsmyndigheten (IMY). Kan vara internt eller externt.

**Informationssäkerhets- och dataskyddsgrupp** - i detta forum sker kommunens samordning och uppföljning av informationssäkerhetsarbetet. Informationssäkerhets- och dataskyddssamordnare (CISO) är sammankallande. Kontaktpersoner för kommunens olika förvaltningar ska ingå och gruppen ska sammanträda regelbundet.

## Uppföljning

Efterlevnaden av informationssäkerhetspolicyn och riktlinjer för informationssäkerhet ska följas upp regelbundet inom Söderköpings kommuns ledningssystem för informationssäkerhet (LIS). Kommunstyrelsen bestämmer närmare hur uppföljningen ska gå till genom antagande av riktlinjer och internkontroll för informationssäkerhet.

För att kunna rapportera uppföljningen enligt Söderköpings kommuns ledningssystem för informationssäkerhet (LIS) behöver kommunala bolag ta fram arbetssätt som möjliggör detta.

Informationssäkerhets- och dataskyddssamordnare (CISO) ska årligen rapportera läge och status gällande informationssäkerhet direkt till kommundirektören och Kommunstyrelsen. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.

Den funktion inom kommunala bolag som har till uppgift att leda, samordna och följa upp informationssäkerhetsarbetet ska årligen rapportera läge och status gällande informationssäkerhet direkt till VD och styrelse.