Policy | 2022-03-15

# Informationssäkerhetspolicy

**Dnr 22/058**

**Fastställd** av Kommunfullmäktige den 2022-05-02

**Ersätter tidigare** *Informationssäkerhetspolicy dnr 2020:254*

**Giltighet**: Tills vidare, för hela kommunkoncernen

**Dokumentansvar**: Kommunstyrelsens kontor / Säkerhetsavdelningen

**Kommunstyrelsen**
Johan Wahlström
Informationssäkerhetsansvarig, Säkerhetsavdelningen
08–52306794
johan.wahlstrom@sodertalje.se

Södertälje kommun

Känslighet - Öppen

## Syfte med informationssäkerhetspolicyn

Denna policy beskriver kommunfullmäktiges övergripande viljeinriktning och mål för informationssäkerhetsarbetet inom Södertälje kommunkoncern.

Syftet med policyn är att ha en gemensam grund att bygga informationssäkerhetsarbetet på och beskriva ansvar och arbetssätt som ska gälla för hela kommunkoncernen. En gemensam grund och tydliga ansvar och arbetssätt är en viktig förutsättning för att över tid upprätthålla en hög informationssäkerhet.

Policyn, samt tillhörande riktlinjer, gäller för alla verksamheter, nämnder och kontor, styrelser och bolag inom kommunkoncernen. Alla användare som hanterar information på något sätt ska efterleva policys och riktlinjer, exempelvis politiker, chefer, medarbetare, kunder/brukare samt externa parter.

## Mål för informationssäkerhetsarbetet

Information är en av de viktigaste tillgångar Södertälje kommunkoncern har och att hantera information är en förutsättning för de flesta av kommunkoncernens verksamheter ska fungera så bra som möjligt.

För att upprätthålla förtroendet från allmänhet, medarbetare, uppdragsgivare och samarbetsparter, behöver all information behandlas på ett tillförlitligt sätt i enlighet med de egenskaper som anges nedan. Detta oavsett om informationen behandlas muntligt, skriftligt eller digitalt.

Det övergripande målet med kommunkoncernens informationssäkerhetsarbete är att bedriva ett långsiktigt och systematiskt informationssäkerhetsarbete som utgår från etablerade standarder (SS-EN ISO/IEC 27001) och utformas i enlighet med MSB:s rekommendationer.
Informationssäkerhetsklassificering ska göras för all information som hanteras digitalt, med stöd av SKR:s verktyg Klassa. Resultatet ska ligga till grund för att välja rätt skyddsnivå för att säkerställa nödvändigt skydd utifrån egenskaperna för informationssäkerhet:

- Konfidentialitet - att åtkomst till kan begränsas till endast behöriga, personer och system.
- Riktighet - att informationen är tillförlitlig, korrekt och fullständig
- Tillgänglighet - att informationen är nåbar i förväntat utsträckning av de med rätt behörighet
- Spårbarhet - att specifika aktiviteter som rör informationen kan spåras, exempelvis ändringar och radering av information, bör finnas för känslig information och är i många fall nödvändigt för att uppnå de tre ovanstående egenskaperna

## Ansvar för informationssäkerhetsarbetet

- **Kommunfullmäktige** uttrycker i denna policy sin övergripande viljeinriktning för kommunkoncernens informationssäkerhetsarbete.
- **Kommunstyrelsen** ansvarar för att samordna och följa upp kommunkoncernens informationssäkerhetsarbete. I detta ingår att säkerställa att organisation och resurser finns för att driva arbetet, samt att besluta om gemensamma riktlinjer.
- **Nämnder och styrelser** ansvarar för informationsägande och är personuppgiftsansvariga för respektive verksamhet. De ska också säkerställa att informationssäkerheten upprätthålls inom sina verksamheter och att policy och riktlinjer följs, samt i förekommande fall kompletteras utifrån förutsättningar för den specifika verksamheten.
- **Stadsdirektören** har det samlade ansvaret för kommunkoncernens informationssäkerhetsarbete.

- **Kontorschef och VD** ansvarar för att säkerställa sitt interna informationssäkerhetsarbete följer gällande policy och riktlinje, samt att nödvändiga resurser och roller finns utpekade inom sin organisation.
- **Informationssäkerhetsansvarig,** som hör till säkerhetsavdelningen, har det operativa ansvaret för att driva och följa upp kommunkoncernens informationssäkerhetsarbete. Denne har också ansvaret att ta fram förslag till policy och riktlinjer, samt underliggande regler och anvisningar, samt stöttar bolag och kontor vid behov.
- **Säkerhetschef** beslutar om underliggande anvisningar.

## Informationssäkerhet, IT-säkerhet och Cybersäkerhet

***Informationssäkerhet*** omfattar all information som kommunkoncernen på något sätt hanterar, oavsett vilken form den finns i, alltså information som är muntlig och skriftlig samt information som lagras i IT-system. En god informationssäkerhet säkerställer att bara rätt personer kommer åt informationen (konfidentialitet), att informationen över tid är tillförlitlig, fullständig och inte förändras (riktighet) samt att informationen går att nå och använda av behöriga personer (tillgänglighet).

Grunden för informationssäkerhetsarbetet är administrativa åtgärder, det vill säga kända och förankrade styrdokument och riskanalyser, samt god kompetens hos alla medarbetare. Även vissa tekniska åtgärder ingår i informationssäkerheten. En övergripande väl förankrad säkerhetskultur är grunden för att upprätthålla en god säkerhet, både generellt och särskilt när det gäller informationssäkerhet. Inom kommunkoncernen finns det övergripande ansvaret för att driva och följa upp arbetet medinformationssäkerhet hos Säkerhetsavdelningen. I det löpande arbetet har respektive kontorschef och VD ansvar för att informationssäkerheten upprätthålls.

***IT-säkerhet*** är avgränsat till digital information som lagras i verksamhetssystem, på servrar, datorer, mobiltelefoner och som skickas via nätverk. IT-säkerheten skyddar denna digitala information med en kombination av tekniska åtgärder (exempelvis kryptering och lösenordsskydd) och andra åtgärder som vidtas för att skydda kommunkoncernens IT-miljö. Även administrativa åtgärder kommer in. I dagsläget ligger ansvaret för IT-säkerhet på respektive systemägare och informationsägare, och om det inte tydligt delegerats, på respektive kontorschef och VD, med möjlighet till stöd från kommunkoncernens IT-organisation.

***Cybersäkerhet*** är ett annat begrepp som blir allt vanligare, och det avser den säkerhet som behövs (både informationssäkerhet och IT-säkerhet) för att skydda kommunkoncernens verksamheter mot cyberhot, vilket definieras som antagonistiska hot mot vår information och/eller IT-miljö. Då cybersäkerhet består av en kombination av informationssäkerhets- och IT-säkerhetsåtgärder och har ett tydligt fokus på antagonistiska hot ligger ansvaret för samordning av detta på Säkerhetsavdelningen.

## Informationssäkerhetsklassificering

All information inom kommunkoncernen behöver informationssäkerhetsklassificeras och denna klassning ska ligga till grund för val av adekvata skyddsåtgärder i relation till risker. Informationen ska bedömas med stöd av gällande riktlinje för Informationsklassificiering, och verksamhetskritisk information ska prioriteras, samt information som kommer att behandlas i molntjänst, eller i annan lösning utanför kommunkoncernens egen miljö.

## LIS – Ledningssystem för Informationssäkerhet

Södertälje kommunkoncerns arbete med informationssäkerhet ska följa denna policy. För att göra detta på ett strukturerat sätt och för att underlätta för de olika verksamheterna, tas under 2022 ett

Ledningssystem för informationssäkerhet (LIS) fram. Detta beskriver närmare hur arbetet ska bedrivas för att uppnå en hög informationssäkerhet.

## Personuppgifter

För information där även personuppgifter behandlas ska denna information hanteras enligt gällande dataskyddslagstiftning.

## Molntjänster och tjänsteköp

För att möta de förväntningar som ställs på Södertälje kommunkoncern är det nödvändigt att nyttja moderna digitala plattformar, som molntjänster eller andra slags tjänsteköp inom IT-området. Detta för att möjliggöra för olika verksamheter att på ett snabbt, enkelt och flexibelt sätt kunna anpassa verktyg och arbetssätt utifrån samhällets krav, behov och efterfrågan.
En av de lösningar som kommer att behöva nyttjas är olika molntjänster och andra IT-tjänster. För att säkerställa att Kommunkoncernen använder sådana tjänster på rätt sätt med bibehållen informationssäkerhet ska följande punkter alltid följas.

***Vid nyttjande av molntjänster och tjänsteköp ska kommunkoncernen:***

- Beakta lagar, avtal och krav innan dessa tjänster nyttjas.
- Arbeta proaktivt med risk- och sårbarhetsanalyser, och genomföra konsekvensbedömning av tjänster innan användningen påbörjas.
- Ständigt utveckla och förbättra metoder, riktlinjer och övriga stöd för att på ett säkert sätt kunna nyttja molntjänster och tjänsteköp.
- Kontinuerligt utbilda medarbetare i såväl arbetssätt som informationssäkerhet.
- Säkerställa att informationen alltid kan flyttas till annan leverantör, eller tas tillbaka vid händelse som kräver detta.

## Giltighet och revidering

Denna policy gäller tills vidare och ska revideras vid behov. Informationssäkerhetsansvarig ansvarar för uppföljning av policy, samt att ta initiativ till revidering.
Policyn kommer att kompletteras med nödvändiga riktlinjer, som där det är möjligt ska vara gemensamma för kommunkoncernen, samt med anvisningar som beslutas på tjänstemannanivå.