

# Policy för Informationssäkerhet

<b>Beslutsdatum</b>	2025-09-25	<b>Dokumenttyp</b>	Policy
<b>Beslutad av</b>	Kommunfullmäktige	<b>Dokumentägare</b>	Chef Avd Demokrati och säkerhet
<b>Diarienummer</b>	KS/2025:330	<b>Giltighetstid</b>	Tillsvidare

## Innehållsförteckning

<b>1</b>	<b>Bakgrund</b> .....	<b>3</b>
<b>2</b>	<b>Grundläggande principer</b> .....	<b>4</b>
	Analysera informationssäkerhet.....	4
	Utforma informationssäkerhet .....	4
	Implementera informationssäkerhet.....	4
	Följa upp och förbättra .....	5
	2.1 Definition.....	5
<b>3</b>	<b>Uppföljning</b> .....	<b>6</b>
<b>4</b>	<b>Översyn och revidering</b> .....	<b>6</b>

# 1 Bakgrund

I en digital tid förändras medborgarnas behov, beteenden och förväntningar i takt med den digitala utvecklingen. För att vara relevant som kommun måste verksamheten möta dessa förväntningar, men det innebär dock att stora mängder data, inklusive känslig information om allt från enskilda individer och dess personuppgifter till samhällskritiska funktioner, skickas, bearbetas och lagras. Det krävs god informationssäkerhet för att bygga motståndskraft och skydda information från obehörig åtkomst, manipulation och förlust, det gäller både vid oavsiktlig och medveten handling. Samtidigt behöver det säkerställas att behöriga användare har åtkomst till korrekt och fullständig information. En god informationssäkerhet är särskilt viktigt för att undvika ekonomiska förluster för kommunen och potentiella hot mot kommuninvånarens fri- och rättigheter.

Då medborgaren står i centrum för kommunens arbete är personuppgifter kommunens enskilt största och mest skyddsvärda informationstillgång. Arbetet med informationssäkerhet står därför i nära relation till data- och integritetskyddsarbetet, som säkerställer skyddet för den personliga integriteten och de grundläggande mänskliga rättigheterna. Medveten styrning och ledning av dessa områden skapar förutsättningar att nyttja digitaliseringen på bästa sätt i strävan att utveckla verksamheten och öka nyttan för medborgarna.

Kommunens informationssäkerhetsarbete styrs och utgår från:

- Lagar, förordningar och föreskrifter
- Kommunens egna krav på prestanda och kvalitet
- Avtal som har koppling till informationssäkerhet

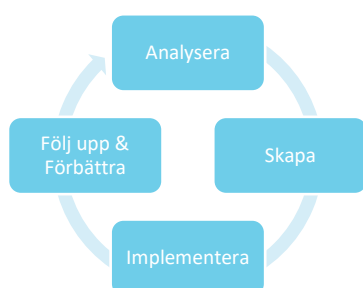
Syftet med kommunens informationssäkerhetsarbete är att säkerställa att:

- Lagar, förordningar och föreskrifter efterlevs
- Ingångna avtal är kända och följs
- Informationsförsörjningen är säker och effektiv för verksamheten
- Informationssäkerhet bibehålls även vid krissituationer
- Information klassas och hanteras med sekretess
- Organisation, rutiner, infrastruktur och systemstöd finns för skydd av känslig (verksamhetskritisk) information och data
- Medarbetare har kännedom om regler, ansvar och befogenheter samt aktivt rapporterar avvikelser
- Kraven för informationssäkerhet integreras i organisationens verksamhetsprocesser, kontroll- och revisionsarbete sker löpande, samt att verksamheten åtar sig att ständigt arbeta med förbättringar inom området

## 2 Grundläggande principer

Denna policy kommer att vara en del av kommunens ledningssystem för informationssäkerhet (LIS) som bygger på den senaste versionen av standarden ISO/IEC 27001 och informationssäkerhetsarbetet ingår som en del i kommunens övergripande ”Handlingsplan för trygghet och säkerhet i Tyresö kommun” som fastställs inför varje ny mandatperiod. Policyn avser att beskriva övergripande definitioner och ramar för kommunens informationssäkerhetsarbete. Hur policyns intentioner ska tolkas i detalj och följas beskrivs i underordnade styrdokument som ska spänna över kommunens samtliga nämnders ansvarsområden. Informationssäkerhetspolicyn omfattar all verksamhet i Tyresö kommun, dess bolag och upphandlade leverantörer/utförare utan undantag.

Kommunen är en komplex organisation med viktiga samhällsuppdrag och därför finns ett grundläggande behov av ett informationssäkerhetsarbete som bedrivs metodiskt, systematiskt och dokumenterat. Det innebär ett strukturerat och iterativt arbetssätt där organisationen analyserar sina förutsättningar och skapar, implementerar, följer upp och förbättrar sitt LIS.



### **Analysera informationssäkerhet**

Förvaltningarna ska genom ett systematiskt arbete analysera informationssäkerhetsrisker för att säkerställa att informationssäkerheten i verksamheten utformas med utgångspunkt i ett tydligt definierat nuläge.

### **Utforma informationssäkerhet**

Det samlade resultatet från analyserna ska styra hur varje förvaltning utformar handlingsplaner, mål och prioritering sitt informationssäkerhetsarbete.

### **Implementera informationssäkerhet**

Resultatet av informationssäkerhetsarbetet och konstaterade behov av säkerhetsåtgärder ska tas om hand av varje förvaltning på ett riskbaserat sätt

för att prioritera och säkerställa ett systematiskt arbetssätt för informationssäkerhetsarbetet.

## Följa upp och förbättra

Förvaltningsledningen ska årligen ta del av status på det systematiska informationssäkerhetsarbetet på en kommunövergripande nivå vid ledningens genomgång. Förvaltningsledningen fattar sedan beslut om prioriteringar och åtgärder inför nästkommande år.

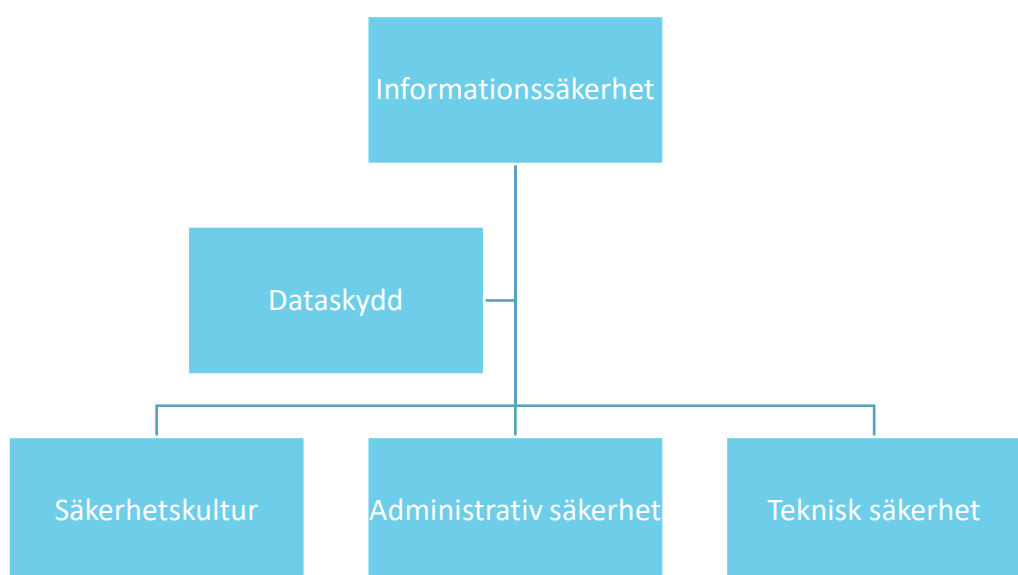
### 2.1 Definition

Med begreppet informationssäkerhet avses alla de säkerhetsåtgärder som behöver vidtas för att

- säkerställa att information är korrekt, tillförlitlig och tillgänglig i förväntad utsträckning och
- hindra att information görs tillgänglig för obehöriga, manipuleras eller förloras, oavsiktligt eller genom medveten handling.

All information som har ett värde för kommunens uppdrag och huvudsyfte att leverera tjänster och service till kommunens invånare omfattas av informationssäkerhetsarbetet. Det gäller även de informationssystem som används för behandling av information och data, som företrädesvis är elektroniska men kan även avse manuell hantering (mappar och akter).

Säkerhetsåtgärderna kan kategoriseras enligt figuren nedan.



**Dataskydd** Arbetet med dataskydd handlar om skydds- och säkerhetsåtgärder som har till uppgift att upprätthålla enskildas fri- och rättigheter vid hanteringen av personuppgifter.

**Säkerhetskultur** är organisationens gemensamma värderingar, beteenden och medvetenhet inom en organisation som påverkar hur medarbetarna ser på och hanterar säkerhet. En stark säkerhetskultur innebär att säkerhetsfrågor prioriteras, risker hanteras proaktivt och att alla i organisationen tar ansvar för att upprätthålla en säker arbetsmiljö och informationshantering.

**Administrativ säkerhet** är organisatoriska åtgärder som policyer, riktlinjer och rutiner som reglerar åtkomst, användning och hantering av information. Även utbildning, revision och avtal är inkluderade.

**Teknisk säkerhet** är tekniska lösningar så som brandväggar, antivirusprogram, kryptering, autentisering och andra säkerhetsverktyg som skyddar mot cyberattacker. Det är även fysiska skyddsåtgärder som låsta dörrar, övervakningskameror, passerkontroll, larm och brandskyddssystem i serverrum och datacenter.

### **3 Uppföljning**

Kommunstyrelsen ska årligen hålla sig informerad om informationssäkerhetsarbetet inom kommunen. Uppföljningen ska baseras på underlag med rekommendationer som koordineras och sammanställs av informationssäkerhetssamordnaren.

### **4 Översyn och revidering**

Detta dokument ska ses över årligen och revideras vid behov.