



ÖVERTORNEÅ  
KOMMUN



# Policy för informationssäkerhet

- Det är mänskligt att fela. För att göra riktigt stora fel krävs en dator.

William E. Vaughan

<b>Dokumenttyp</b>	<b>Ärendenummer</b>	<b>Fastställd</b>	<b>Giltighetstid</b>
Policy	KS 2023/39	2023-02-27	Tills vidare
<b>Dokumentansvarig</b>	<b>Tidigare reviderad</b>	<b>Beslutsinstans</b>	<b>Dokument gäller för</b>
Informationssäkerhets- samordnare	Antagen 2023	Kommun- fullmäktige	Alla anställda

## Innehållsförteckning

<b>1. Informationssäkerhet</b>	<b>1</b>
1.1 <i>Omfattning</i>	1
1.2 <i>Definition</i>	1
1.3 <i>Översiktsbild informationssäkerhet (TR 50)</i>	1
<b>2. Mål</b>	<b>2</b>
2.1 <i>Viljeriktningar</i>	2
2.2 <i>Metodik</i>	2
<b>3. Lagstiftning</b>	<b>3</b>
<b>4. Roller och ansvar</b>	<b>3</b>
<b>5. Uppföljning</b>	<b>5</b>
<b>6. Referenser</b>	<b>6</b>

# 1. Informationssäkerhet

## 1.1 Omfattning

Informationssäkerhetspolicyn är övergripande med mål, inriktning och ansvarsfördelning för Övertorneå kommuns informationssäkerhet. Den är en del av kommunens ledningssystem för informationssäkerhet. Policyn omfattar organisationens samtliga informationstillgångar, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna. Informationssäkerhetspolicyn gäller inte för kommunens bolag, undantaget när de använder sig av kommunens gemensamma informationstillgångar, eller då det finns särskilda behov av samordning.

Informationssäkerhetspolicyn ska kompletteras av verksamhetsspecifika styrdokumentet och riktlinjer.

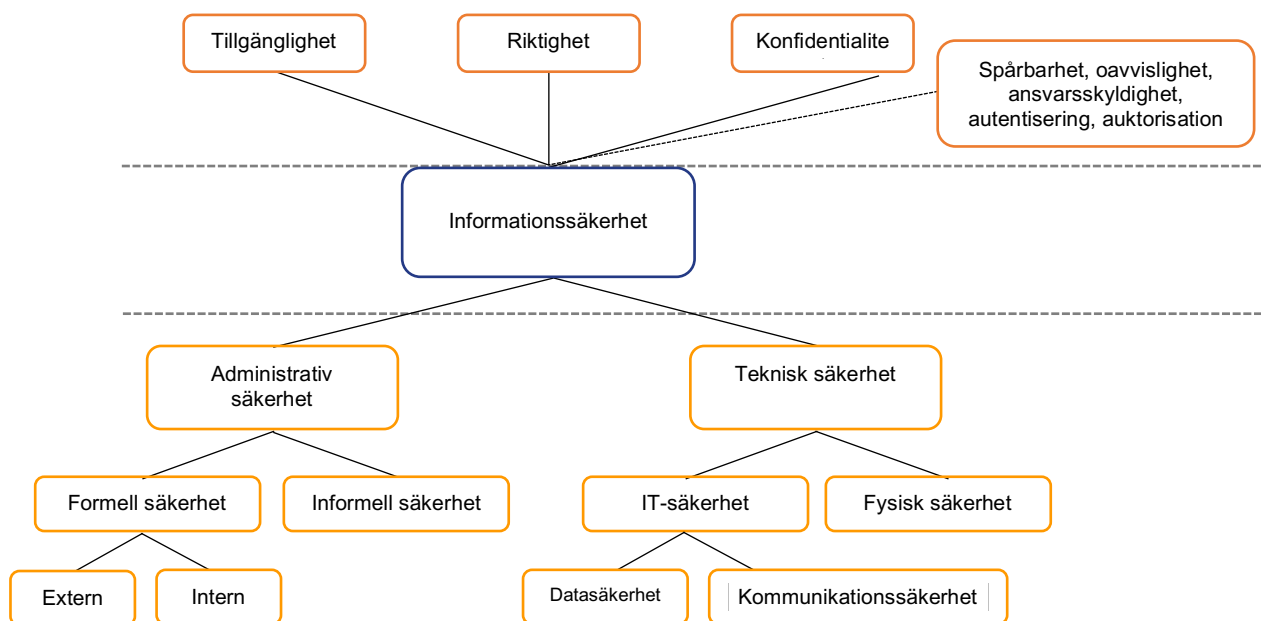
Oavsett om informationen är fysisk, digital eller muntlig ska informationssäkerheten ska vara ett centralt inslag i kommunens arbetssätt. Övertorneå kommun ska beakta särskilt fokus med informationssäkerhet vid kommunens arbete med säkerhetsskydd, krisberedskap samt IT-efterlevnad.

## 1.2 Definition

Informationssäkerhet är de tekniska och administrativa åtgärder som utförs för att skydda en organisations information utifrån:

1. Tillgänglighet, att den alltid finns när den behövs
2. Riktighet, att den alltid är korrekt och inte manipulerad eller förstörd
3. Konfidentialitet, att endast behöriga personer får ta del av den

## 1.3 Översiktsbild informationssäkerhet (TR 50)



Figurens struktur är baserad på och hämtad från SIS-TR 50:2015

## 2. Mål

### 2.1 Viljeriktningar

Kommunen ska uppfylla nuvarande och tillkommande lagkrav, förordningar, föreskrifter samt de avtalsförhållanden som berör kommunen och som kräver ett systematiskt informationssäkerhetsarbete.

Övertorneå kommun ska arbeta systematiskt med informationssäkerhet för att:

- Skydda Övertorneå kommuns medborgare, anställda och samarbetspartners rättigheter i förhållande till dataskydd och personlig integritet
- Minska risken för att sårbarheter i förhållande till informationssäkerhet utnyttjas och arbeta för att motverka informationssäkerhetsrisker i den interna organisationen
- Informationshanteringen är förutsägbar, trygg och likformig i hela kommunen
- Kommunens informationstillgångar är korrekta, tillgängliga och enbart delges till behörig samt att hantering sker på ett spårbart sätt.
- Effektivisera och stödja kommunens pågående digitaliseringsprocess

### 2.2 Metodik

För att uppnå ovanstående viljeriktningar ska Övertorneå kommun:

- Upprätta ledningssystem för informationssäkerhet, LIS som uppfyller de grundläggande kraven på systematiskt informationssäkerhetsarbete enligt ISO/IEC 27000-serien
- Tillämpa ett arbetssätt som stödjer ständiga förbättringar och bygger på en helhetssyn som utgår från information, men som också innefattar processer, människor och teknik
- Arbeta förebyggande, proaktiv och ha förmåga att hantera eventuella incidenter, störningar och kriser
- Följa och samverka med företag, nätverk och myndigheter till exempel MSB, Myndigheten för samhällsskydd och beredskap
- Beakta informationssäkerhet vid upphandling utefter en riskhanteringsprocess
- Samtliga kritiska informationstillgångar informationsklassas
- Återkommande utbilda och öva alla anställda i kommunen för att stärka säkerhetsmedvetandet och utveckla säkerhetskulturen
- Utgå från att alltid hantera kommunens informationstillgångar med försiktighet och vidta säkra och beprövade metoder för informationshantering

### 3. Lagstiftning

- Arbetsmiljölagen (1977:1160)
- Arkivlagen (1990:782)
- Dataskyddsförordningen (Europaparlamentets och rådets förordning 2016/679)
- Dataskyddslagen (Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning)
- Förvaltningslagen (2017:900)
- Kommunallagen (2017:725)
- Lag om behandling av personuppgifter inom socialtjänsten (2001:454)
- Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174, s.k. NIS-direktivet<sup>1</sup>)
- Lag 2006:554 om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
- Lag om offentlig upphandling (2016:1145)
- Offentlighets- och sekretesslagen (2009:400)
- Patientdatalagen (2008:355)
- Skollag 2010:800
- Socialtjänstlag 2001:453
- Säkerhetsskyddslagen (2018:585)
- Säkerhetsskyddsförordning (2018:658)
- Tryckfrihetsförordningen (1949:105)

### 4. Roller och ansvar

Ansvaret för informationssäkerhet följer ordinarie verksamhetsansvar. Detta gäller från kommunledningen till den enskilde medarbetaren, och innebär att den som är ansvarig för en verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet.

**Alla medarbetare oavsett roll och funktion** har ett ansvar att följa Övertorneå kommuns informationssäkerhetspolicy. Varje medarbetare har också ansvar att vara uppmärksam på brister och incidenter rörande informationssäkerhet och meddela sådana till närmsta chef.

**Ytterst ansvarig för informationssäkerhet** är ledning i form av kommunstyrelse och kommunens nämnder med ansvar för verksamhet som bedrivs inom deras respektive verksamhetsområden. Varje nämnd kan vid behov besluta om instruktioner som förtydligar och kompletterar centrala styrdokumentet inom informationssäkerhet.

**Personuppgiftsansvariga** är kommunstyrelsen och övriga nämnder i kommuner. Dessa är ansvariga för hanteringen av personuppgifter och ska utse dataskyddsombud

---

<sup>1</sup> Kommunens informationstillgångar lyder i nuläget inte under NIS-direktivet, NIS1. NIS2 kommer senast den 17 oktober 2024 antas inom svensk lag och kan då komma omfatta kommunens informationstillgångar.

**Dataskyddsbud** har till ansvar att informera och ger råd till den personuppgiftsansvariga organisationen om vilka skyldigheter som gäller enligt dataskyddsförordningen. Ombudet bevakar att reglerna följs och fungerar som kontaktperson för Integritetsskyddsmyndigheten.

**Informationsägare**, äger informationen inom sitt verksamhetsområde och ansvarar för informationens kvalitet samt att hanteringen uppfyller krav på informationssäkerhet.

**Arkivansvarig** är respektive verksamhetschef. Arkivansvarig ser till att informationen hanteras enligt gällande regler; tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen, samt kommunens interna styrdokument.

**Systemägare** har övergripande ansvar för administration, drift och säkerhet för ett informationssystem. Rollen förutsätter förvaltnings- och budgetansvar. Systemägare ska utse systemadministratörer och ansvarar för att systemadministratören har rätt förutsättning för rollen.

**Systemadministratör** är en användare med utökad behörighet i informationssystem och har det funktionella och dagliga ansvaret för system hen administrerar. Systemförvaltaren fungerar i hög grad som systemägarens utförare och ser till systemets funktionalitet samt att planerade eller beslutade aktiviteter genomförs och upprätthålls.

**Säkerhetschefen** ansvarar för att säkerheten i Övertorneå kommuns IT-miljö som tjänster, processer, informationssystem, infrastruktur, verktyg osv är tillräcklig och uppfyller verksamhetens krav, legala krav samt denna informationssäkerhetspolicy och underliggande riktlinjer för informationssäkerhet.

**Informationssäkerhetssamordnare** har det övergripande och strategiska ansvaret att leda, utveckla, samordna och stötta informationssäkerhetsarbetet.

## 5. Uppföljning

Informationssäkerhetssamordnaren ska årligen upprätta en rapportavseende Övertorneå kommuns informationssäkerhetsarbete. Rapporten delges och presenteras till kommundirektörens ledningsgrupp, samtliga nämnder och styrelse. Vartannat genomförs en större informationssäkerhetsanalys som presenteras till kommundirektörens ledningsgrupp. Särskilda skäl, exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.

Övertorneå kommuns Dataskyddsombud ska avrapportera dataskyddsarbetet vid samtliga nämndsmöten en gång per år. Dataskyddsombudet kan vid behov begära att frågan lyfts till kommundirektörens ledningsgrupp.

Kommundirektören kan lyfta frågan om informationssäkerhet/dataskydd under sin informationspunkt vid kommunstyrelsen.

## 6. Referenser

ISO/IEC 27000-serien

<https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/lag-forordning-och-foreskrifter/>

<https://www.informationssakerhet.se/metodstodet/>

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823>

<https://skr.se/download/18.5f94e9591811657edb85f67/1654005694573/Guide-for-tillrackligt-god-informationssakerhet-SKR.pdf>

<https://www.uddevalla.se/download/18.2ae68e5016364b7c4c114dd/1666177825724/Informationss%C3%A4kerhetspolicy.pdf>

<https://sunne.se/globalassets/dokument/7.-kommun-och-politik/kommunfakta/forfattningssamling/samhallsskydd-och-sakerhet/informationssakerhetspolicy-kf-2022-03-21.pdf>