Uppsala kommun

Kommunledningskontoret
**Tjänsteskrivelse till Kommunstyrelsen**

Handläggare:
Robert Reineck

Datum:
2024-01-18

Diarienummer:
KSN-2023-03218

# Riktlinje för informationssäkerhet, dataskydd och cybersäkerhet

## Förslag till beslut

Kommunstyrelsens ordförandeberedning beslutar

1. **att** fastställa förslag till riktlinje för informationssäkerhet, dataskydd och cybersäkerhet i ärendets bilaga 1

## Ärendet

Sedan tidigare finns en riktlinje för informationssäkerhet beslutad av kommunstyrelsen med diarienummer KSN-2019-0350. Syftet med den uppdaterade riktlinjen är att skapa tydligare förutsättningar för ett systematiskt och integrerat arbete med informationssäkerhet, dataskydd och cybersäkerhet i kommunkoncernen.

### Beredning

Ärendet har beretts av kommunledningskontoret.

Ärendet har inga konsekvenser sett ur barn-, jämställdhets- eller näringslivsperspektiv.

### Föredragning

Syftet med riktlinjen är att skapa förutsättningar för ett systematiskt och integrerat arbete med informationssäkerhet, dataskydd och cybersäkerhet samt hur detta ska bedrivas i nämnder och bolagsstyrelser i Uppsala kommun.

Arbetet med informationssäkerhet och cybersäkerhet ska bidra till att kommunkoncernen kan genomföra samtliga uppdrag utan störningar. Det ska även skapa en motståndskraft och förmåga till återhämtning i de fall störningar ändå inträffar. Arbetet med dataskydd handlar om skydds- och säkerhetsåtgärder som har till uppgift att upprätthålla enskildas fri- och rättigheter vid hanteringen av personuppgifter.

Tillgången till information är en förutsättning för en väl fungerande offentlig verksamhet. Med en god informationsförvaltning kan kommunkoncernen hantera information som en värdefull, långsiktig strategisk resurs under informationens hela livscykel. Brister i informationsförvaltningen kan få mycket allvarliga konsekvenser.

Förslaget till den uppdaterade riktlinjen syftar bland annat till att

- tydliggöra dataskydd och cybersäkerhet som viktiga delar i arbetet med informationssäkerhet
- fastställa att det ska finnas en funktion för informationssäkerhet inom kommunkoncernen
- fastställa att det ska finnas en dataskyddssamordnare för varje nämnd och bolag.

En följd av att kommunfullmäktige beslutar om riktlinjen är att den då omfattar hela kommunkoncernen inklusive de kommunala bolagen vilket är av vikt för att uppnå syftet med informationssäkerhetsarbetet.

**Ekonomiska konsekvenser**

Beslutet innebär inga ytterligare ekonomiska konsekvenser då funktionen för informationssäkerhet redan är etablerad och i arbete sedan 5 år. Detsamma gäller för dataskyddssamordnarna som har verkat för respektive nämnd och bolag sedan 4 år. Det systematiska arbetet med informationssäkerhet, dataskydd och cybersäkerhet i sig självt syftar till att identifiera risker vars åtgärder kan vara kostnadsdrivande. Sådana åtgärder hanteras inom befintlig ram.

**Beslutsunderlag**

- Tjänsteskrivelse daterad 18 januari 2024.
- Bilaga 1, Förslag till riktlinje för informationssäkerhet daterad 18 januari 2024.

Kommunledningskontoret

| | |
|---|---|
| Joachim Danielsson<br>Stadsdirektör | Ola Hägglund<br>Ekonomidirektör och bitr. stadsdirektör |

Uppsala kommun

**Normerande styrdokument**

Beslutsfattare:
Kommunfullmäktige

Dokumentansvarig:
CIO

Datum:
2024-01-18

Diarienummer:
KSN-2023-03218

# Riktlinje för informationssäkerhet, dataskydd och cybersäkerhet

Policy

**Riktlinje**

Rutin

Vägledning

# Innehåll

# Inledning

Arbetet med informationssäkerhet och cybersäkerhet ska bidra till att kommunkoncernen kan genomföra samtliga uppdrag utan störningar. Det ska även skapa en motståndskraft och förmåga till återhämtning i de fall störningar ändå inträffar. Arbetet med dataskydd handlar om skydds- och säkerhetsåtgärder som har till uppgift att upprätthålla enskildas fri- och rättigheter vid hanteringen av personuppgifter.

Tillgången till information är en förutsättning för en väl fungerande offentlig verksamhet. Med en god informationsförvaltning kan kommunkoncernen hantera information som en värdefull, långsiktig strategisk resurs under informationens hela livscykel. Brister i informationsförvaltningen kan få mycket allvarliga konsekvenser.

Därför måste kommunkoncernen skydda informationen så att:

- den alltid finns när den behövs (tillgänglighet)
- den går att lita på, att den är korrekt och inte heller manipulerad eller förstörd (riktighet)
- endast behöriga personer får ta del av den (konfidentialitet).

Ett bristande skydd kan leda till att skada uppstår på samhällets skyddsvärden:

- människors liv och hälsa
- samhällets funktionalitet
- demokrati, rättssäkerhet och mänskliga fri- och rättigheter
- ekonomi och miljö
- nationell suveränitet.

Ett ändamålsenligt skydd uppnås genom säkerhetsåtgärder som är anpassade efter de risker som påverkar kommunkoncernens förmåga att genomföra sitt uppdrag.

För att åstadkomma detta behövs ett systematiskt informationssäkerhetsarbete som inkluderar perspektiven dataskydd och cybersäkerhet. Hur detta tar sig uttryck inom Uppsala kommun beskrivs i denna riktlinje.

Informationssäkerhetsarbetet bidrar också till att:

- verksamheten bedrivs ändamålsenligt och resurseffektivt
- informationen och rapporteringen om verksamheten och ekonomin är tillförlitlig och rättvisande
- verksamheten efterlever lagar, regler, avtal med mera.

Arbetet med informationssäkerhet utförs i enlighet med Ledningssystem för informationssäkerhet (ISO/IEC 27001:2023), och Riktlinjer för informationssäkerhetsåtgärder (ISO/IEC 27002:2022). Arbetet har till uppgift att bevara förväntad konfidentialitet, riktighet och tillgänglighet för Uppsala kommuns informationstillgångar.

## Syfte

Riktlinjen beskriver gemensamma förutsättningar för ett systematiskt, riskbaserat och integrerat arbete med informationssäkerhet inom hela kommunkoncernen.

## Omfattning

Riktlinjen gäller hela kommunkoncernen, både nämnder och bolagsstyrelser.

# Arbetet med informationssäkerhet

## Genomförande

Arbetet med informationssäkerhet, dataskydd och cybersäkerhet ska:

- stärka kommunkoncernens förmåga att identifiera sårbarheter, risker och hot mot de egna informationstillgångarna och deras skyddsbehov
- skapa förutsättningar att minska dessa risker till en acceptabel nivå
- utformas så att rätt information är tillgänglig för rätt person vid rätt tillfälle
- skapa en robust hantering av information genom att vara förebyggande och proaktivt
- skapa en förmåga att upptäcka, hantera och lära av de avvikelser och störningar som kan inträffa
- vara känt och tillämpat i hela organisationen
- ge medarbetare förutsättningar för fortlöpande kompetenshöjning för ökat säkerhetsmedvetande
- tydliggöra vad ledningens och övriga organisationens ansvar innebär
- vara en integrerad del av kommunkoncernens planering, budgetering, genomförande och uppföljning
- vara systematiskt – genom styrning, kontroll och uppföljning enligt standarden Ledningssystem för informationssäkerhet (SS-ISO/IEC 27001:2023)
- integreras i verksamhetens styrdokument enligt standarden Riktlinjer för informationssäkerhetsåtgärder (SS-ISO/IEC 27002:2022)
- utformas enligt MSBFS 2020:7 och senaste version av CIS Controls avseende cybersäkerhet
- utgå ifrån de råd och modeller som tas fram av myndigheter med särskilda uppdrag inom informationssäkerhetsområdet
- bedrivas aktivt i samverkan med Sveriges kommuner och regioner (SKR)
- följas upp löpande och förbättras i takt med omgivningens förändrade förutsättningar

## Definitioner och begrepp

**Informationssäkerhet** – bevarande av konfidentialitet, riktighet och tillgänglighet hos information. Används i riktlinjens sammanhang som samlingsbegrepp och inkluderar då dataskydd och cybersäkerhet.

**Dataskydd** – avser de principer och regler som gäller till skydd för fysiska personer vid behandling av deras personuppgifter.

**Cybersäkerhet** – all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.

**IT-säkerhet** – del av informationssäkerhet avgränsad till it-resurser. It-resurser kan vara nätverk, servrar, hårdvara, mjuk/programvara, mobila enheter, klienter och brandväggar.

**Informationstillgång** – information som är av värde för organisationen och även de resurser som hanterar den. Det kan handla om människor, papper, mjukvara, hårdvara och immateriella tillgångar som rykte och förtroende.

## Lagbestämmelser och krav

Några av de mest framträdande kraven som normerar arbetet med informations-säkerhet återfinns i följande standarder och författningar:

**Dataskyddsförordningen GDPR**-

Dataskyddsförordningen ställer krav på systematiskt informationssäkerhetsarbete med målet att skydda enskildas grundläggande fri- och rättigheter.

**NIS-direktivet (EU) 2016/1148**

EU-direktiv och tillkommande nationell författning som syftar till att upprätthålla kontinuiteten i samhällsviktiga tjänster samt begränsa hoten mot de nätverks- och informationssystem som den samhällsviktiga tjänsten är beroende av.

**Tryckfrihetsförordningen (1949:105) och Offentlighets- och sekretesslagen (2009:400) (OSL)**

Systematiskt informationssäkerhetsarbete som tryggar offentlighetsprincipen och förhindrar röjandet av uppgifter som omfattas av sekretess är en förutsättning för dessa lagar.

**Säkerhetsskyddslagen (2018:585)**

Information som är sekretessbelagd med hänsyn till Sveriges säkerhet ges ett särskilt skydd genom säkerhetsskyddslagen.

**Arkivlagen (1990:782)**

En viktig uppgift med många kopplingar till informationssäkerhet är att över tid säkra riktigheten hos allmänna handlingar och även säkra tillgänglighet.

**HSL-FS 2016:40**

Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården föreskriver om informationssäkerhet i de delar av Uppsala kommun som omfattas av patientdatalagen (2008:355).

**MSBFS 2020:6**

Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter. Gäller enbart statliga myndigheter men är en utgångspunkt även för Uppsala kommuns arbete med informationssäkerhet.

**MSBFS 2020:7**

Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter. De utgör tillsammans med ISO/IEC 27002:2022 och CIS Controls version 8 grunden för Uppsala kommuns arbete med cybersäkerhet.

**Ledningssystem för informationssäkerhet (ISO/IEC 27001:2023) och Riktlinjer för informationssäkerhetsåtgärder (ISO/IEC 27002:2022)**. Dessa standarder beskriver ett systematiskt och riskbaserat arbete med informationssäkerhet med stöd av ett ledningssystem för informationssäkerhet. Uppsala kommuns arbete med informationssäkerhet ska utgå från dessa standarder.

**CIS Controls**

Är en uppsättning säkerhetsåtgärder som i nuvarande version är fördelade över 18 övergripande förmågor. Förmågorna är grundläggande för att kunna stoppa, begränsa, upptäcka och åtgärda cyberangrepp.

## Funktioner och roller

Inom kommunkoncernen ska följande finnas:

**Funktionen för informationssäkerhet**

Funktionens syfte är att samordna kommunkoncernens systematiska och strategiska arbete med informationssäkerhet, dataskydd och cybersäkerhet. Funktionen organiseras inom kommunledningskontoret.

**Dataskyddssamordnare**

För varje nämnd och bolag inom Uppsala kommunkoncern ska det finnas en eller flera dataskyddssamordnare som koordinerar det verksamhetsnära arbetet med dataskydd och informationssäkerhet.

## Ansvar

Alla medarbetare i kommunkoncernen har ett eget ansvar för informationssäkerheten utifrån sitt uppdrag.

Alla verksamhetschefer ansvarar för att den egna verksamheten arbetar med informationssäkerhet utifrån riktlinjen.

Kommunstyrelsen ansvarar för att stödja och följa upp kommunkoncernens samtliga verksamheter när det gäller informationssäkerhet. Utifrån riktlinjen normerar kommunstyrelsen arbetet med informationssäkerhet ytterligare.

# Relaterade dokument

- Reglemente för kommunstyrelsen och övriga nämnder i Uppsala kommun
- Reglemente för intern kontroll inom Uppsala kommun och dess helägda bolag
- Policy för digital transformation
- Riktlinje för riskhantering