ESLÖVS KOMMUN

# RIKTLINJE FÖR INFORMATIONSSÄKERHET

Dokumentet är antaget av kommunstyrelsen att gälla från och med den 15 mars 2023. Det riktar sig till hela kommunen. Ses över för revidering senast mars 2026. Kontaktperson: Informationssäkerhetssamordnare.

# Innehåll

# 1 Inledning

Information är en förutsättning för Eslövs kommuns arbete. Information anskaffas, lagras, kommuniceras och bearbetas i olika former. En del av Eslövs kommuns information kan omfattas av sekretess eller beröra samhällsviktig verksamhet. Det kan innebära stora negativa konsekvenser för Eslövs kommun om information går förlorad eller inte finns till hands när den behövs. Ifall information röjs för obehöriga kan det leda till obehag för den enskilde Och/eller få konsekvenser för vår förmåga att bedriva verksamhet.
Organisationens krav på informationssäkerhet baseras på interna krav i verksamheten samt externa krav i form av lagstiftning.
Medborgarna ska kunna känna tillit till att information inom Eslövs kommun hanteras korrekt och har erforderligt skydd.

Informationen ska skyddas enligt följande principer:

- Konfidentialitet- endast behörig personal får tillgång till information.
- Riktighet- information ska vara korrekt.
- Tillgänglighet- informationen ska vara tillgänglig.

Patientsäkerhet är ett prioriterat område för Eslövs kommun inom informationssäkerhet och är en förutsättning för att uppnå kvalitet och säkerhet i vården samt för skydda den personliga integriteten för patienter. Det systematiska informationssäkerhetsarbetet i Eslövs kommun har sin grund i standarden för informationssäkerhet, ISO/IEC 27000.

## 1.1 Syfte

Riktlinjen utgår från Eslövs kommuns policy för systematiskt säkerhetsarbete och anger hur Eslövs kommun arbetar med informationssäkerhet. Riktlinjen baseras på standarden för informationssäkerhet SS-ISO/IEC 27000.

## 1.2 Omfattning

Riktlinjen omfattar all information oavsett om den behandlas manuellt, digitalt eller automatiserat och oberoende vilken form informationen är i.

### 1.3 Övergripande process

Process visar övergripande de olika delarna för att uppnå en god informationssäkerhet. Alla delar av organisationen berörs av processen.


### 1.4 Övergripande styrdokument

Policy för systematiskt säkerhetsarbete beskriver Eslövs kommuns syn på säkerhetsarbetet och de övergripande principer som gäller. Policyn är antagen av kommunfullmäktige. Riktlinje för informationssäkerhet konkretiserar säkerhetspolicyn avseende grundläggande delar inom informationssäkerhet. Riktlinjen beslutas av kommunstyrelsen. Rutiner, instruktioner och anvisningar för informationssäkerhet anger hur arbetet ska bedrivas i praktiken utifrån säkerhetspolicy och riktlinjerna. Dessa beslutas enligt bestämmelserna i Riktlinje för styrdokument.

## 2 Grundläggande principer

Inom Eslövs kommun ska ett systematiskt och långsiktigt informationssäkerhetsarbete bedrivas.
Eslövs kommuns informationstillgångar ska identifieras, klassificeras och tilldelas en lämplig skyddsnivå med utgångspunkt i:

- att de finns tillgängliga när de behövs (tillgänglighet),
- att de är korrekta (riktighet)
- att obehöriga inte kan få tillgång till dem (konfidentialitet).

Eslövs kommun ska, utifrån återkommande riskanalyser och inträffade incidenter, avgöra hur risker ska hanteras och vidta

nödvändiga åtgärder för att upprätthålla rätt skyddsnivå för informationen.
För att uppnå målet med informationssäkerheten ska arbetet omfatta samtliga delar av administrativ respektive teknisk säkerhet.
I enlighet med vad som gäller för övrig verksamhet, är ansvaret för informationssäkerheten kopplat till det delegerade verksamhetsansvaret. Det innebär att varje anställd som är ansvarig för en verksamhet eller får ett delegerat verksamhetsansvar också är ansvarig för att informationssäkerheten upprätthålls och efterföljs i denna verksamhet.

# 3 Informationsägare

Yttersta ansvaret för information och hur vi ska hantera den beslutar informationsägaren om. Det är även informationsägaren som beslutar ifall informationen får användas i olika IT- system.
Varje förvaltningschef är informationsägare för den information som skapas, behandlas och upprättas inom förvaltningen om det inte finns en annan fastställd informationsägare, t.ex. anställdas information vilken HR-chef är informationsägare för.

Tabellen nedan är tänkt som ett stöd och förtydligande.

| | |
|---|---|
| Information om kommunikation för hela kommunen. | Kommunikationschef |
| Information om anställda och annan information avseende HR. | HR - chef |
| Information om barn och vuxna som berör förskola, grundskola eller gymnasium eller annan eftergymnasial utbildning. | Förvaltningschef Barn och Utbildning |
| Information om brukare, patienter eller vårdtagare inom vård och omsorg. | Förvaltningschef Vård och omsorg |
| Information om personer som deltar eller medverkar i kultur och fritidsaktiviteter samt evenemang mm. | Förvaltningschef Kultur och Fritid |

| | |
|---|---|
| Information om våra fastigheter, IT system, nätverk mm | Förvaltningschef Miljö och Samhällsbyggnad |
| Ekonomisk information som rör kommunen på ett övergripande plan. | Ekonomichef |

# 4 Organisation

För att uppnå och bibehålla en god informationssäkerhet ska ansvar inom informationssäkerhet definieras och tilldelas.

## 4.1 Övergripande ansvar för informationssäkerheten

**Kommunfullmäktige**
Kommunfullmäktige beslutar om Eslövs kommuns informationssäkerhetspolicy, samt om långsiktiga mål för informationssäkerhetsarbetet.

**Kommunstyrelsen**
Kommunstyrelsen har det övergripande ansvaret för informationssäkerhet i Eslövs kommun. Kommunstyrelsen beslutar om Eslövs kommuns riktlinje för informationssäkerhet. Kommunstyrelsen ska minst en gång per år, vid ledningens genomgång, informeras om status på informationssäkerhetsarbetet.

**Kommundirektören**
Kommundirektören ansvarar för att informationssäkerhetsarbetet bedrivs effektivt så att informationssäkerhetsmålen kan uppnås. Kommundirektören beslutar om vem som ska vara informationsägare för informationstillgångar som är gemensamma för kommunen.

**Informationssäkerhetssamordnare**
Informationssäkerhetssamordnaren ansvarar för att leda, utveckla, samordna och övergripande följa upp informationssäkerhetsarbetet inom Eslövs kommun. I ansvaret ingår att förvalta riktlinjen för informationssäkerhet, kommunövergripande instruktioner och anvisningar samt målen för informationssäkerhet. I uppdraget ingår omvärldsbevakning och kontakt med externa myndigheter i informationssäkerhetsfrågor.

# 5 Personalsäkerhet

Alla som arbetar i Eslövs kommun ska kunna förstå sitt ansvar för och bidra till att hantera och skydda Eslövs kommuns informationstillgångar. Personalens kunskaper och insikt i informationssäkerhetsrisker och hur dessa hanteras är en viktig del i ett effektivt informationssäkerhetsarbete. Informationssäkerhetsåtgärder ska vara en del av anställningsprocessen och stå i proportion till verksamhetens krav, klassificeringen av information som den anställde ska ges behörighet till och de risker som kan förekomma. Detsamma gäller under hela anställningen tills dess att anställningen upphör. Bakgrundskontroll kan förekomma för en del tjänster.

# 6 Hantering av tillgångar

Eslövs kommun hanterar stora mängder information som har olika typer av skyddsvärde. Det är exempelvis personuppgifter, patientuppgifter, information om upphandlingar, risk- och sårbarhetsanalyser och sekretessbelagd information. Informationsobjekt ska identifieras och klassificeras för att möjliggöra en lämplig skyddsnivå med utgångspunkt i att informationen finns tillgänglig när den behövs (tillgänglighet), att den är korrekt (riktighet) samt att obehöriga inte kan få tillgång till informationen (konfidentialitet).

# 7 Åtkomst till information

All tillgång till information inom Eslövs kommun ska styras med hjälp av administrativa och tekniska skyddsåtgärder. Detta för att endast behöriga får tillgång till informationen. För att anses behörig ska man vara beroende av informationen för att kunna utföra sitt arbete. Behörigheter till information och system ska baseras på arbetsuppgifter och organisatorisk tillhörighet samt följas upp regelbundet. Varje användares identitet ska kunna verifieras och alltid vara spårbar till en fysisk person. För att kunna säkerställa korrekt användning av behörigheter behöver i vissa fall loggning och uppföljning genomföras. Informationsägaren beslutar om vilka säkerhetsåtgärder som krävs för åtkomst till information baserat på genomförd informationsklassificering och riskanalys.

# 8 Fysisk och miljörelaterad säkerhet

En riskanalys ska ligga till grund för det fysiska skalskydd som ska finnas för att skydda informationstillgångar. Utformning och styrka för skalskyddet ska vara anpassat till skyddsvärdet. I skyddet ska behovet av brandskydd, skalskydd, avbrottsfri kraft, kylsystem, kablagesäkerhet med mera, utvärderas med stöd av expertis inom området. De skyddsåtgärder som införs ska testas regelbundet för att verifiera att de har avsedd effekt.

# 9 Driftsäkerhet

I syfte att säkerställa säker och pålitlig tillgång till information, ska administration, drift och underhåll av system ske på ett strukturerat och systematiskt sätt, enligt en fastställd modell för systemförvaltning. System som stödjer samhällsviktig eller verksamhetskritisk verksamhet ska driftövervakas kontinuerligt för att minimera avbrott och andra informationssäkerhetsincidenter. När en verksamhet inom Eslövs kommun köper en tjänst från en extern part eller förlägger drift av system hos en sådan, ska samma krav för informationssäkerhet gälla som när driften hanteras i egen regi. System och utrustning som kan drabbas av skadlig kod, ska skyddas.

# 10 Kommunikationssäkerhet

Skyddsåtgärder ska finnas för att skydda information och anslutna tjänster mot obehörig åtkomst. Vid kommunikation över öppna nätverk ska särskilda skyddsåtgärder vidtas för att garantera konfidentialitet och riktighet för data som överförs. Detsamma gäller för att upprätthålla krav på tillgänglighet till nätverkstjänster och anslutna enheter. Loggning och övervakning ska tillämpas för att registrera och upptäcka åtgärder som kan påverka informationssäkerheten.

# 11 Anskaffning, utveckling och underhåll av system

Informationssäkerhetskraven, vid upphandling, ny- och vidareutveckling av system, i egen regi eller i samverkan med samarbetspartner, ska analyseras och definieras utifrån en dokumenterad informationsklassificering och riskanalys. Informationssäkerhetskrav och säkerhetsåtgärder ska återspegla värdet av den information som ska hanteras och den negativa påverkan på verksamheten som brist på tillräckligt skydd kan leda till. Identifiering av

informationssäkerhetskrav ska integreras i tidiga faser då det kan leda till mer verkningsfulla och kostnadseffektiva lösningar. Ett system ska, innan det tas i drift, ha godkänts ur säkerhetssynpunkt av informationsägaren eller informationsägarna.

# 12 Leverantörsrelationer

Leverantörers åtkomst till Eslövs kommuns tillgångar ska vara reglerat i avtal. Det omfattar leverantörer som kan få åtkomst till, behandlar eller kommunicerar information som ägs av Eslövs kommun eller tillhandahåller infrastrukturtjänster. Avtalsansvarig ansvarar för att regelbundet granska och revidera avtalade leveranser för att säkerställa att avtalet följs samt att informationssäkerhetsincidenter hanteras korrekt. Det är av stor vikt att Eslövs kommun har kontroll över och insyn i de säkerhetsaspekter där känslig eller kritisk information är nåbar, bearbetas eller förvaltas av en extern leverantör.

# 13 Informationssäkerhetsincidenter

Eslövs kommun ska arbeta proaktivt för att förebygga informationssäkerhetsincidenter. Inträffade informationssäkerhetsincidenter ska hanteras skyndsamt för att minimera skadorna i verksamheten med hjälp av kontinuitetsplaner. Identifierade sårbarheter ska åtgärdas skyndsamt i syfte att undvika incidenter. Informationssäkerhetsincidenter där anmälningsskyldighet finns enligt lag eller förordning, ska anmälas till ansvarig myndighet. Informationssäkerhetsincidenter ska sammanställas årligen i syfte att förbättra arbetet med informationssäkerhet och att förebygga framtida incidenter.

# 14 Kontinuitet

Det är viktigt att fastställa hur länge avbrott är acceptabla för verksamheten. För att hitta rätt ambitionsnivå ska juridiska krav samt verksamhetens behov av tillgång till information dokumenteras i informationsklassningen och riskanalys ska genomföras. Kontinuitetsplanerna ska innefatta reservrutiner och övriga åtgärder som kan vidtas för att säkerställa verksamhetens kontinuitet. Om verksamheten är beroende av leverantör ska även leverantören ingå i arbetet med kontinuitet och krav på leverantörens ansvar och förmåga ska dokumenteras.

# 15 Uppföljning och efterlevnad

Kommunstyrelsen har det övergripande ansvaret för informationssäkerheten inom Eslövs kommun och därmed även ansvar för uppföljning. Varje förvaltning är ansvarig för informationssäkerheten inom sin verksamhet och ska:

- Löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.
- Granska sin informationssäkerhet och baserat på genomförda granskningar och identifierade avvikelser vidta skyddsåtgärder.

För att säkerställa att styrande dokument efterföljs, ska uppföljningar genomföras såväl årligen som när det inträffar väsentliga händelser som påverkar informationssäkerheten. Dessa kan initieras av kommundirektören eller informationssäkerhetssamordnaren.