

Gemensamma anvisningar för riskhantering av information

Diarienummer: KS-2026/00250
Paragraf: § 82
Beslutsinstans: Kommunens ledningsgrupp
Beslutsdatum: 2026-09-03

Informationsklassning: KO: R1: T1
Dokumentansvarig: Informationssäkerhetssamordnare
Giltighetstid: Tills vidare

Föregående diarienummer:
Föregående beslutsdatum:
Föregående beslutsinstans:
Föregående paragraf:

Inledning

Denna gemensamma anvisning gäller för samtliga förvaltningar inom Motala kommun och återger ett gemensamt sätt att tillämpa kommunens arbetssätt för riskhantering av information. Anvisningen riktar sig till alla som hanterar kommunens information och är en viktig del av att säkerställa att kommunens resurser används på ett tryggt och säkert sätt.

Mål

Dessa gemensamma anvisningar är underordnad kommunens informationssäkerhets- och dataskyddspolicy och ska bidra till att kommunen uppnår fastställda mål. Målen omfattar i synnerhet att systematiska riskanalyser och klassificeringar ska genomföras för att säkerställa en ändamålsenlig och korrekt nivå av skydd för kommunens informationstillgångar samt IT-system.

Detta styrdokument utgör ett led i kommunens arbete med att efterleva cybersäkerhetslagen (2025:1506) och Myndigheten för civilt försvars föreskrifter om krav på riskhantering.

Syftet med riskhantering

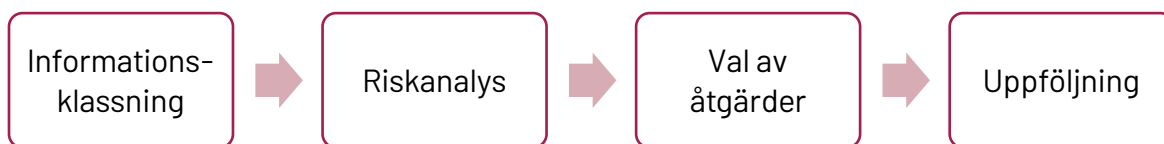
Arbetet med riskhantering inkluderar informationsklassning, riskanalys och val av åtgärder. Syftet med informationsklassningar, riskanalyser och säkerhetsåtgärder är att säkerställa att informationen skyddas i enlighet med dess betydelse för verksamheten och gällande lagstiftning.

Informationsklassning fastställer informationens skyddsbehov och ökar medarbetares medvetenhet om konsekvenserna av bristande skydd, medan riskanalyser identifierar och värderar hot och sårbarheter mot dessa tillgångar. Resultatet från informationsklassningar och riskbedömningar används som underlag för att välja ändamålsenliga och proportionerliga säkerhetsåtgärder, så att skyddet anpassas både till informationens skyddsbehov och verksamhetens aktuella risker. Genom denna process kan organisationen prioritera resurser på ett effektivt sätt, minska risken för informationssäkerhetsincidenter och säkerställa att informationssäkerheten upprätthålls över tid.

Metodstöd för riskhantering

För att underlätta implementeringen av kommunens arbete med riskhantering finns ett metodstöd som syftar till att stödja verksamheterna i arbetet med informationsklassning, riskanalys och val av säkerhetsåtgärder. Metodstödet har utformats på ett vägledande sätt för att beskriva hur riskhanteringsprocessen ska genomföras i praktiken och för att säkerställa ett enhetligt och systematiskt arbetssätt inom hela kommunen.

Övergripande riskhanteringsprocess



Informationsklassning

Informationsklassning innebär att kommunen bedömer hur skyddsvärd information är och vilka konsekvenser som kan uppstå om skyddet brister i aspekterna konfidentialitet, riktighet eller tillgänglighet. Syftet är att säkerställa att information hanteras på en nivå som motsvarar dess värde och betydelse för verksamheten. Klassningen utgör grunden för beslut om skyddsåtgärder och bidrar till att upprätthålla en hög och enhetlig nivå av informationssäkerhet inom kommunen.

Riskanalys

En riskanalys är en metod för att identifiera, bedöma och värdera risker som är förknippade med information som analyseras (även kallat analysobjekt). Syftet med en riskanalys är att identifiera situationer där kommunen riskerar att inte uppnå fastställda mål, att tillhandahålla beslutsunderlag för val av nödvändiga säkerhetsåtgärder samt att öka medvetenheten om risker relaterade till det aktuella analysobjektet.

Val av åtgärder

Valet av åtgärder innebär att kommunen, med utgångspunkt i genomförda informationsklassningar och riskanalyser, fastställer vilka säkerhetsåtgärder som krävs för att hantera identifierade risker och uppfylla krav på konfidentialitet, riktighet och tillgänglighet. Åtgärderna ska vara ändamålsenliga och proportionella mot de bedömda skyddsbehoven.

Uppföljning

Informationsklassningar och riskanalyser ska regelbundet följas upp för att säkerställa deras aktualitet. Detta då informationens betydelse för verksamheten kan förändras över tid och påverka valet av säkerhetsåtgärder. Förvaltningarnas uppföljning utgör även underlag för en övergripande uppföljning av kommunens informationssäkerhetsarbete som informationssäkerhetssamordnaren genomför.

Ansvar och roller

Förvaltningschef – ansvarar för att riskhanteringen följs upp inom ramen för den årliga uppföljningen av förvaltningens informationssäkerhetsarbete samt för att fatta beslut om förvaltningsspecifika styrdokument avseende riskhantering.

Verksamhets- och enhetschef – är informationsansvarig och ansvarar för att information inom verksamheten informationsklassas, att riskanalyser genomförs samt att beslut fattas om lämpliga skyddsåtgärder utifrån verksamhetens behov och informationens känslighet. När informationen hanteras i ett system ställer informationsansvarig, utifrån klassningen och riskanalys, krav på systemmiljön.

Systemägare - Systemägaren tar emot och samordnar de krav som berörda informationsansvariga ställer, ansvarar för att riskanalys av systemmiljön genomförs samt beslutar om de säkerhetsåtgärder som vidtas i miljön. Systemägaren säkerställer att drift och förvaltning av system skyddas med lämpliga och proportionella säkerhetsåtgärder under hela systemets livslängd. Systemägarens uppgifter beskrivs närmare i kommunens systemförvaltningsmodell. Systemägaren ska informera berörda informationsansvariga om brister i systemets cybersäkerhet.

Informationssäkerhets- och dataskyddskoordinator – har till uppgift att leda, driva och samordna informationssäkerhets- och dataskyddsarbetet inom sin förvaltning på operativ nivå. Koordinatoren ska informeras och bistå som stöd i förvaltningens riskhanteringsarbete samt verka för att detta bedrivs i enlighet med fastställda riktlinjer, anvisningar och metoder.

Informationssäkerhetssamordnare – har det övergripande ansvaret för att leda, utveckla, samordna och följa upp kommunens informationssäkerhetsarbete. Samordnaren ska stödja samtliga förvaltningar i alla faser av riskhanteringsprocessen samt verka för att informationssäkerhetsarbetet bedrivs i enlighet med fastställda styrdokument.

Dataskyddsombud – Dataskyddsombudet ansvarar för att informera och ge råd till den personuppgiftsansvariga organisationen om tillämpliga skyldigheter enligt dataskyddsförordningen (GDPR). Dataskyddsombudet ska övervaka efterlevnaden av dataskyddsförordningen, fungera som kontaktperson gentemot registrerade och Integritetsskyddsmyndigheten samt stödja kommunens förvaltningar i dataskyddsfrågor.

Klassningsmodell

Kommunens klassningsmodell bygger på MCF:s metodstöd för informationssäkerhet och används för att bedöma konsekvenser av bristande konfidentialitet, riktighet och tillgänglighet. Bedömningen görs på en femgradig skala utifrån konsekvenskategorier som ekonomisk skada, verksamhetspåverkan, lagefterlevnad, förtroendeskada, påverkan på liv och hälsa samt individers fri- och rättigheter. Syftet är att skapa en enhetlig och riskbaserad klassning av information.

Riskacceptanskriterier

Vid genomförandet av en riskanalys ska följande skala användas för att bedöma om en risk kan accepteras eller inte samt för att ange på vilken nivå beslut om riskacceptans får fattas.

Riskenivå	Kan accepteras av	Krav för att risken ska få accepteras
Låg (L)	Informationsansvarig respektive systemägare	Dokumenteras i riskanalysen med kort motivering
Medel (M)	Informationsansvarig respektive systemägare	Dokumenteras i riskanalysen med motivering till varför risk accepteras istället för att åtgärdas samt vilka alternativ (undvika, överföra, reducera) som övervägts och valts bort
Hög (H)	Förvaltningschef	Motivering enligt ovan. Redovisas till informationssäkerhetssamordnare för kommunens samlade riskbild
Extremt hög (EH)	Informationsägare (kommunstyrelse eller nämnd)	Presumption mot acceptans: risken ska i första hand åtgärdas. Om acceptans ändå väljs krävs skriftlig motivering, omedelbar redovisning till samordnaren samt en plan för att sänka risken till lägre nivå

Systemstöd

Systemstödet stödjer hela riskhanteringsprocessen för information och möjliggör en spårbar samt dokumenterad hantering av risker samt beslut inom hela kommunen. Systemstödet ska bland annat användas under klassningar och som stöd vid val av åtgärder.

Relaterade dokument

- Metodstöd för riskhantering av information
- Gemensamma anvisningar för systemförvaltning
- Informationssäkerhets- och dataskyddspolicy
- Riktlinjer för informationssäkerhet