

Informationssäkerhets- och dataskyddspolicy

Diarienummer:	KS2025-00299
Paragraf:	§
Beslutsinstans:	Kommunfullmäktige
Beslutsdatum:	2025-12-08
Informationsklassning:	K:0 R:1 T:1
Dokumentansvarig:	Gemensam ledningsförvaltning
Giltighetstid:	Tills vidare
Föregående diarienummer:	KS-2019/00116
Föregående beslutsdatum:	2019-06-10
Föregående beslutsinstans:	Kommunfullmäktige
Föregående paragraf:	§86

Informationssäkerhets- och dataskyddspolicy

Inledning och bakgrund

Denna informationssäkerhets- och dataskyddspolicy redovisar Motala kommuns övergripande mål, principer och inriktning för arbetet med informationssäkerhet och dataskydd samt hur ansvaret är fördelat. Policyn omfattar all information, inklusive personuppgifter, som hanteras inom kommunen. Med information avses all information oberoende av var och hur informationen hanteras, oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Kommunens arbete med informationssäkerhet och dataskydd ska bedrivas på ett systematiskt, formaliserat och riskbaserat sätt. Genom etablerade rutiner för incidenthantering säkerställs att potentiella säkerhetshot kan förebyggas, identifieras, hanteras och reduceras.

Om informationssäkerhet

Information finns och hanteras i alla kommunens verksamheter vilket gör information till en central tillgång. Denna information rör exempelvis verksamheter, medarbetare, tjänster, ekonomi samt relationer med kommuninvånare, företag och det civila samhället. Oavsett om informationen är i form av text, ljud, bild, film eller annan media, och oavsett om den hanteras med hjälp av IT, på papper eller muntligt, är det av största vikt att informationen skyddas och hanteras korrekt för att uppfylla lagkrav och säkerställa en hög informationssäkerhet i verksamheterna.

Informationssäkerhet handlar om att skydda information. Det görs genom att skapa och upprätthålla lämpliga rutiner och skydd för att garantera att informationen hanteras på rätt sätt. Informationssäkerhet uppnås genom att följande grundläggande principer efterföljs:

- **Konfidentialitet:** Information ska inte vara tillgänglig eller avslöjas för obehöriga.
- **Riktighet:** Information ska vara korrekt, tillförlitlig och inte manipulerad.
 - **Spårbarhet:** När det är en förutsättning eller ett lagkrav ska förändringar i informationen kunna spåras och återskapas.
- **Tillgänglighet:** Information ska vara åtkomlig och användbar för behörig när den behövs.

Om dataskydd

Dataskydd utgör en del av informationssäkerheten och ett extra skydd för personuppgifter utifrån specifika dataskyddsregler. Dataskyddsreglerna grundar sig i de mänskliga rättigheterna. Alla människor har rätt till respekt för privat- och familjeliv och till skydd av sina personuppgifter. Alla verksamheter i Motala kommun som hanterar personuppgifter måste följa dataskyddsförordningen (GDPR) och kompletterande svenska regler på dataskyddsområdet. Regelverket innebär bland annat att de grundläggande principerna behöver följas, att respektive behandling stöds på en rättslig grund och att individerna (de registrerade) informeras om hur deras personuppgifter hanteras.

Vid behandling av personuppgifter ska

- uppgifterna behandlas på ett *lagligt, korrekt och öppet* sätt i förhållande till den registrerade,
- de samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (*ändamålsbegränsning*),
- de vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering*),
- de vara korrekta och om nödvändigt uppdaterade (*korrekthet*),
- de inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas (*lagringsminimering*),
- de behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*),

De personuppgiftsansvariga myndigheterna inom kommunen ska ansvara för och kunna visa att principerna ovan efterlevs (*ansvarsskyldighet*).

Mål med informationssäkerhet och dataskydd

Informationssäkerhet och dataskydd bidrar till att kommunen når dess övergripande visioner, strategier och mål. Inom Motala kommun är målet med informationssäkerhets- och dataskyddsarbetet att skapa en trygg, robust och effektiv informationshantering som stödjer kommunens mål och som möter kommuninvånarens förväntningar. Vi strävar efter en säkerhetskultur där ansvar för informationssäkerhet och dataskydd är tydligt definierat och stöds av ledningen, vilket ger våra medarbetare kunskap och resurser för att skydda information, känsliga uppgifter och personuppgifter utifrån sammanhängande risk.

Rätt information ska finnas tillgänglig för rätt mottagare vid rätt tidpunkt. Kommunens informationstillgångar ska således uppnå egenskaper i form av tillgänglighet, riktighet och konfidentialitet. Detta säkerställs bland annat genom våra strategier för kryptografi, åtkomstkontroll och tillgångsförvaltning. Genom systematiska riskanalyser och klassificeringar säkerställer vi att information och IT-tjänster skyddas i enlighet med säkerhetskrav.

Vårt informationssäkerhets- och dataskyddsarbete syftar till att främja förtroendet för vår informationshantering, stärka den personliga integriteten och bidra till en digitalt hållbar framtid där vi möter interna och externa intressenters krav och behov.

Tekniska-, fysiska-, administrativa och mänskliga säkerhetsåtgärder

Informationssäkerhet såväl som dataskydd ska vara integrerade delar av verksamheten och ska omfatta både tekniska säkerhetsåtgärder, såsom data- och systemsäkerhet samt fysiskt skydd av IT-infrastruktur och byggnader, och administrativa åtgärder som styrdokument, processer, riskanalyser, externa avtal, och revision. Alla som hanterar informationstillgångar och personuppgifter har ett ansvar att upprätthålla skyddet för dessa och att värna de registrerades personliga integritet, varför mänskliga säkerhetsåtgärder i form av exempelvis utbildnings- och informationsinsatser, återrapportering och övningar behöver vidtas.

Ansvar och roller

Inom Motala kommun ligger det ytterst övergripande ansvaret hos det politiska styret i form av Kommunfullmäktige, Kommunstyrelse och nämnder. Ansvaret för informationssäkerhet och dataskydd följer sedan det delegerade verksamhetsansvaret vilket innebär att ansvaret sträcker sig från kommunledning ner till varje enskild medarbetare inom kommunen. Alla anställda inom kommunen har således ett ansvar för att upprätthålla informationssäkerheten och dataskyddet och uppmärksamma samt rapportera eventuella brister. Den som är ansvarig för en specifik verksamhet har också ansvaret för informationssäkerheten och dataskyddet inom den verksamheten så att den information inklusive de personuppgifter som hanteras inom verksamheten skyddas på ett korrekt sätt.

Roller

Nedan följer en beskrivning av informationssäkerhets- och dataskyddsansvaret för särskilda organ och roller. Ansvar och tillhörande ansvarsområden för respektive roll beskrivs utförligare i riktlinjer för informationssäkerhet.

Informationsägare och personuppgiftsansvariga – det yttersta övergripande ägarskapet för informationssäkerheten och dataskyddet ligger

hos den politiska ledningen i form av Kommunstyrelse och nämnder. De är informationsägare samt personuppgiftsansvariga inom sina respektive områden och ska därmed arbeta systematiskt för att säkerställa att informationen skyddas enligt gällande författningar, policy och riktlinjer.

Kommunfullmäktige – fastställer den informationssäkerhets- och dataskyddspolicy som ska gälla för kommunen. Genom antagande av informationssäkerhets- och dataskyddspolicy fastställer kommunfullmäktige mål och viljeriktning för kommunens informationssäkerhetsarbete.

Kommunstyrelsen – ansvarar för att kommunens informationssäkerhets- och dataskyddspolicy följs och för samordning av informationssäkerhets- och dataskyddsarbetet i kommunen. Kommunstyrelsen ansvarar för att riktlinjer för informationssäkerhet och dataskydd fastställs, hålls aktuella och följs upp. Kommunstyrelsen ska fastställa en övergripande handlingsplan för informationssäkerhets- och dataskyddsarbetet.

Respektive nämnd – är ytterst ansvarig för informationssäkerheten och dataskyddet inom dess respektive verksamhetsområde. Respektive nämnd ska säkerställa att antagna riktlinjer och gemensamma anvisningar efterlevs samt tillse att tillräckliga anvisningar och rutiner finns i verksamheten. Respektive nämnd är personuppgiftsansvarig för dess verksamhet och utser Dataskyddsombud.

Säkerhetsskyddschef – har det övergripande ansvaret att leda, utveckla och samordna Motala kommuns säkerhetsskyddsarbetet.

Informationssäkerhetssamordnare – har det övergripande ansvaret att leda, utveckla, samordna och följa upp informationssäkerhetsarbetet. Informationssäkerhetssamordnaren ska arbeta i samråd med säkerhetsskyddschef och övriga i kommunens strategiska styrgrupp för informationssäkerhets- och dataskydd.

Dataskyddsombud – ansvarar för att informera och ge råd till den personuppgiftsansvariga organisationen om vilka skyldigheter som gäller enligt dataskyddsförordningen. Dataskyddsombudet ska också övervaka efterlevnaden av reglerna och fungera som kontaktperson för dels de registrerade, dels Integritetsskyddsmyndigheten.

Förvaltningschefer – ansvarar för att informationssäkerhetsarbetet följs upp i nämnd och att minst en informationssäkerhets- och dataskyddskoordinator utnämns för respektive förvaltning. Förvaltningschefer tar beslut om förvaltningsspecifika anvisningar och rutiner avseende informationssäkerhet och dataskydd.

Verksamhets- och enhetschefer – är informationsansvariga och ska säkerställa att arbetet med informationssäkerhet och dataskydd bedrivs i enlighet med denna policy samt tillhörande riktlinjer inom respektive

verksamhetsområde. Rutiner beslutas på verksamhets- eller enhetsnivå av ansvarig chef. Det åligger varje verksamhetsansvarig att tillhandahålla medarbetarna den information och utbildning som krävs för att uppnå en god informationssäkerhet och ett gott dataskydd samt för att bidra till en säkerhetskultur hos medarbetarna.

Systemägare – är ansvarig för informationen i systemet. Systemägaren ansvarar för beslut om vidareutveckling och avveckling av system.

Systemförvaltare – har det funktionella och dagliga ansvaret för system samt informationen i system. Systemförvaltare fungerar i hög grad som systemägarens utförare och ser till systemets funktionalitet, samt att beslutade aktiviteter genomförs och upprätthålls.

Informationssäkerhets- och dataskyddskoordinator – har till uppgift att leda, driva, utveckla och samordna informationssäkerhets- och dataskyddsarbetet för respektive förvaltning på operativ nivå. Informationssäkerhets- och dataskyddskoordinatorer är en del av den operativa informationssäkerhets- och dataskyddsgruppen.

Medarbetare – alla medarbetare inom verksamheten har en del i ansvaret för verksamhetens informationssäkerhet och dataskydd. Varje anställd ska i eget arbete följa riktlinjer för informationssäkerhet och dataskydd samt eventuella verksamhetsspecifika anvisningar.

Informationssäkerhets- och dataskyddsorganisation

För att kommunledningen ska kunna fatta välgrundade beslut om budget och fastställa styrdokument och i förlängningen att informationssäkerhets- respektive dataskyddsarbetet ska kunna bedrivas effektivt ska det finnas en informationssäkerhets- och dataskyddsorganisation. Organisationen möjliggör att informationssäkerhetsarbetet planeras och följs upp på strategisk nivå samt samordnas och drivs igenom på operativ nivå.

Styrgruppen för informationssäkerhet- och dataskydd ska planera och följa upp arbetet med informationssäkerhet och dataskydd på strategisk nivå. Gruppen ska ansvara för att bereda strategiska frågor, initiativ och beslutsunderlag till kommunens ledningsgrupp.

På operativ nivå ska informationssäkerhets- och dataskyddsgruppen driva och samordna informationssäkerhets- och dataskyddsarbetet. Den titel vars uppgifter är att leda, driva, utveckla, samordna och följa upp informationssäkerhets- och dataskyddsarbetet för respektive förvaltning, kallas informationssäkerhets- och dataskyddskoordinator. Minst en informationssäkerhets- och dataskyddskoordinator ska utses för att arbeta för respektive förvaltning.

I Riktlinjer för informationssäkerhet respektive Riktlinjer för dataskydd finns en mer utförlig beskrivning av informationssäkerhets- och dataskyddsansvarets olika nivåer i kommunen samt detaljer om informationssäkerhets- och dataskyddsorganisationen.

Uppföljning och revidering

För att säkerställa en god informationssäkerhet och ett gott dataskydd ska efterlevnaden av informationssäkerhets- och dataskyddspolicyn samt underliggande styrdokument följas upp regelbundet inom kommunens ledningssystem för informationssäkerhet (LIS).

Rapportering sker i form av ledningens genomgång vilket är ett tillvägagångssätt som följer av ISO/IEC 27001:2022. Ledningens genomgång sker årligen genom att kommunens informationssäkerhetssamordnare rapporterar status gällande informationssäkerhet till kommunstyrelsen, kommundirektören och kommunens ledningsgrupp. Statusrapporten består av aktuella informationssäkerhetsrisker, omvärldsbevakning, statistik över informationssäkerhetsincidenter, resultat från kontroller samt revisioner, behov av förbättringar och resurser för att upprätthålla en ändamålsenlig och ett systematiskt informationssäkerhetsarbete. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar. Vid behov granskas informationssäkerhetsarbetet av oberoende part.

Avseende uppföljning av dataskyddet genomförs sådan genom oberoende granskning av dataskyddsombudet eftersom det ingår i dess formella rollbeskrivning.