Vägledning för informationssäkerhet

Östhammars kommun

Målgrupp	Chefer, alla kontor och verksamheter
Avsändare	Kommunledningskontoret, Digitalisering och projektledning
Dokumentansvarig	Informationssäkerhetssamordnare
Framtagen	2024-11-28
Reviderad	2026-03-05

ÖSTHAMMARS KOMMUN
– EN DEL AV ROSLAGEN

Innehåll

1 Om vägledningen och dess sammanhang

Denna vägledning bygger på kommunövergripande och verksamhetsnära analyser av informationssäkerhet och resultatet av interna och externa revisioner. Det övergripande målet med informationssäkerhetsarbetet är att skydda kommunens verksamheter mot avbrott och minimera risken för att information hanteras på ett felaktigt sätt. Syftet med dataskyddsarbetet är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, i linje med dataskyddsförordningen (GDPR)[1].

Vägledningen bygger på EU-direktiv, lagar och förordningar som styr informationssäkerhet, cybersäkerhet och dataskydd. Från och med 2025 är informationssäkerhet även en integrerad del i Östhammars kommuns ledningssystem. Lagar som styr informationssäkerhet- och cybersäkerhet är NIS2/cybersäkerhetslagen och CER-direktivet 2025.

Styr- och stöddokument:

- Program för informationssäkerhet - inbegriper dataskydd och cybersäkerhet[2].
- Handlingsplaner för informationssäkerhet respektive dataskydd
- Vägledning för chefer (detta dokument)
- Kommungemensamma rutiner, stödanvisningar och stödmaterial för informationssäkerhet och dataskydd (uppdateras löpande)

Programmet ger den politiska viljeinriktningen och mål för informationssäkerhetsarbetet, vilket motsvarar policy i standard för informations- och cybersäkerhet (ISO 27000-serien[3]). I handlingsplanerna finns tidsatta aktiviteter för stärkt informationssäkerhet och dataskydd.

Samtliga av kommunens chefer med verksamhetsansvar ska arbeta i riktning mot det mål som uttrycks i Program för informationssäkerhet, innebärande att samtliga chefer ska:

- Införa ett systematiskt och riskbaserat arbetssätt för informationssäkerhetsarbete. Detta innebär att väsentliga risker identifieras och hanteras med lämpliga riskhanteringsåtgärder.
- Tillse att verksamheten har erforderlig kompetens inom området.
- Tillse att uppkomna incidenter som medför eller kan medföra betydande störningar adresseras och inrapporteras på tillbörligt vis.
- Tillse att informationssäkerhetsplanering är en beståndsdel i verksamhetens samlade kontinuitetsplanering.
- Tillse att verksamheten klassificerar information utifrån konfidentialitet, riktighet och tillgänglighet (KRT)

För samtliga ovanstående punkter ska informationssäkerhetsteamet bistå verksamheten med vägledning och operativt stöd. Denna vägledning är en del i det.

[1] https://www.imy.se/verksamhet/dataskydd/
[2] Cybersäkerhet: Informationssäkerhet avseende indirekta och direkta, externa beroenden och hot som finns i ett större och mer komplext digitalt ekosystem än inom den egna organisationen eller samhället.
[3] https://www.sis.se/iso27001/dettariso27001/ledningssystem-och-systematiskt-arbete-enligt-iso-27000/

Vägledningens innehåll motsvarar riktlinjer i ISO 27000-serien och är skriven som ett stöd för kommunens chefer och nyckelpersoner som arbetar med att stärka informationssäkerheten inom sina respektive områden. Internt finns även rutiner, stödmaterial och information som beskriver det sammanhållna, systematiska och riskbaserade arbetssättet samt verktyg som underlättar arbetet. Riktad mot externa intressenter finns samlad information om hur kommunen arbetar med informationssäkerhet och dataskydd.

Innehållet uppdateras löpande för att möta verksamhetsbehov, externa krav och rådande omvärldsläge. Styrdokument och information ska alltid finnas tillgängliga på kommunens externa webbplats och intranät (Ines). Vägledning, stöd, verktyg, etc. finns endast på Ines.

2 Vad som menas med informationssäkerhet

Informationssäkerhet handlar om att ha kontroll över information och flöden. Information ska ges rätt skydd enligt kriterierna konfidentialitet, riktighet och tillgänglighet (KRT). I det ingår att säkerställa spårbarhet för skyddsvärd och känslig information. Informationssäkerhet omfattar all verksamhet och all information inom kommunen, oavsett om den finns i datorer, i ett telefonsamtal eller på ett papper. Arbetet med informations-, cyber-, IT-säkerhet och dataskydd ska samordnas på ett sätt som säkerställer ett bra skydd och säker hantering av information genom hela dess livscykel.

Cybersäkerhetsarbetet handlar om att bedriva ett proaktivt arbete för att öka säkerhetsmedvetenheten och på olika sätt skydda verksamheten mot oönskade avbrott. Förutsättningarna att upptäcka och avvärja olika hot och IT-attacker behöver löpande förbättras. Genom förebyggande åtgärder kan digital information ges ett ändamålsenligt skydd. Om det värsta ändå skulle inträffa kan kommunens förberedande arbete (inbegriper bl.a. krisberedskap, kontinuitetsplanering, samarbete och övningar) underlätta en effektiv krishantering som minimerar skadeverkningarna av en händelse.

Dataskyddsarbetet ska bedrivas enligt dataskyddsförordningen (GDPR). GDPR gäller i hela EU och syftar bl.a. till att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet inom EU och EES *inte* hindras. Då alla verksamheter följer GDPR och kommunens arbetssätt med dataskydd kan ett fullgott skydd av personuppgifter uppnås.

Krav på IT-säkerhet: Med verksamheternas klassning av information, riskarbete och informationssäkerhetskrav följer krav på IT-säkerhet, teknisk och fysisk säkerhet.
I styrdokument för IT-säkerhet ska det framgå hur IT-säkerheten möter dessa säkerhetskrav. IT-centrum[4] ansvarar för att det finns IT-säkerhetspolicy och IT-säkerhetsregler att följa.

[4] IT-centrum är kommunens IT-förvaltning. Den styrs av en it-nämnd gemensam för fem kommuner i Uppland - Knivsta, Tierp, Älvkarleby, Heby och Östhammar. Välkommen till IT-Centrum.

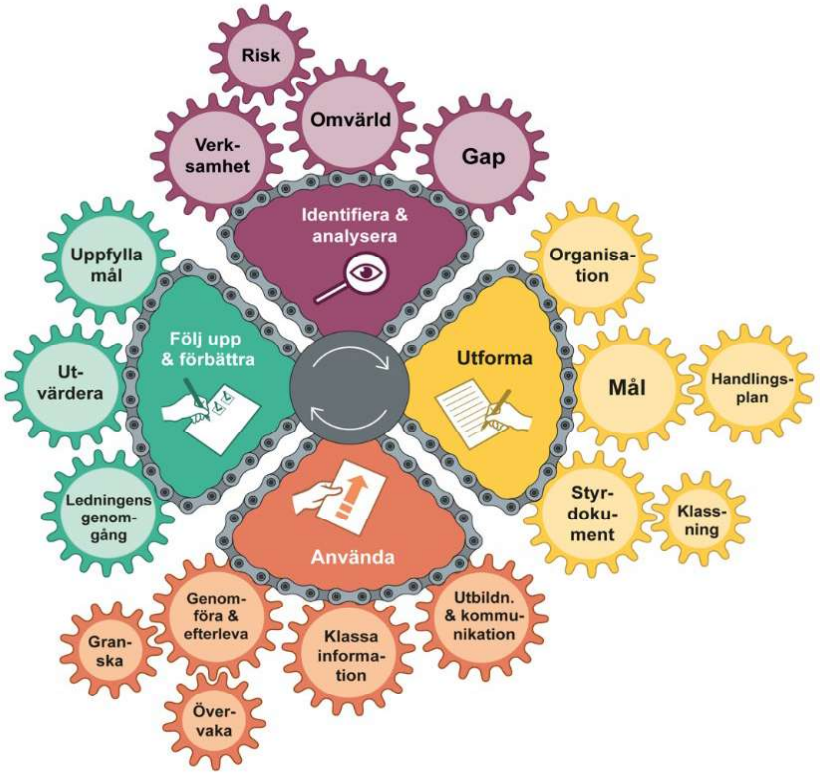
3 ISO-standards i 27000-serien och metodstöd

Kommunen har som riktmärke att följa ISO-standards i 27000-serien för att underlätta arbetet med informationssäkerhet. Det betyder *inte* att kommunen har som ambition att certifiera sig, inte heller att alla chefer och nyckelpersoner behöver sätta sig in i alla detaljer.

Informationssäkerhetsteamet använder Myndigheten för civilt försvar (MCF) metodstöd ”Ledningssystem för informations-säkerhet[5]” som ett verktyg för att införa gemensamma arbetssätt, upprätthålla informationssäkerheten på en god nivå och successivt förbättra den. Metodstödet bygger på ISO 27001/ 27002, men är lättare att följa än ISO-standards.

Genom att använda metodstödet får vi ett arbetssätt som liknar andra organisationers. Det gör det enklare att tillsammans möta olika hot i vår omvärld. Som kommun kan vi även möta externa krav som ställs i samband med att vi vill ingå olika samarbeten, t.ex. Sveriges kommuners handslag för välfärdsutveckling genom digitalisering[6], eller ansöka om medel från staten och EU. Metodstödet underlättar också lagefterlevnad, ger en hint om vad en granskning kan innebära och vilka krav som vi förväntas uppfylla vid en tillsyn.

Arbetssättet skapar förutsättningar för att information ska vara korrekt, autentisk och gå att nå när den behövs samt att enbart behöriga personer får del av skyddsvärd och känslig information. I förlängningen bidrar det till en säker digitalisering och till att upprätthålla trygghet och förtroende hos medarbetare, medborgare, nationella och internationella intressenter.



[5] MSB:s metodstöd för systematiskt informationssäkerhetsarbete
https://www.mcf.se/sv/amnesomraden/informationssakerhet-och-cybersakerhet/arbeta-systematiskt-med-informationssakerhet-och-cybersakerhet/metodstod-for-informationssakerhetsarbete/

[6] Läs mer om Handslag för digitalisering på SKR (Sveriges Kommuners och Regioners webbplats).
https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/handslagfordigitalisering.6728.html

4 Verksamhetsplanering, informationssäkerhet och kontinuitet

4.1 Informationssäkerhet i verksamhetsplanering

Informationssäkerhet är en del av kommunens totala verksamhetsplanering och riskhantering. Alla verksamheter behöver bedriva ett systematiskt arbete med informationssäkerhet och dataskydd. I det ingår att analysera verksamhetens behov och möta externa krav. Centralt är också att klassa information, genomföra riskarbete och se till att information skyddas och hanteras på ett säkert sätt genom hela sin livscykel - i olika system och sammanhang.

4.2 Kontinuitetsplanering

Varje verksamhet behöver ha en ”plan B” – kontinuitetsplan – som beskriver vem som gör vad och hur information kan skyddas och hanteras på ett säkert sätt under ett oönskat avbrott. Ett avbrott kan t.ex. uppstå när ett kritiskt verksamhetssystem av någon anledning inte går att nå eller använda. Avbrottet kan vara kort- eller långvarigt, det är därför bra att kontinuitetsplanera med olika tidsaspekter. All verksamhet är viktig, men kritiska och samhällsviktiga verksamheter/system/tjänster bör prioriteras. Notera att ”plan B” aldrig får innebära en sämre informationssäkerhet än i normalläget, säkerheten behöver säkerställas även vid manuella arbetssätt. Kontinuitetsplaner bör regelbundet testas och övas.

4.3 Intressentanalys

Intressentanalys är en betydelsefull del i informationssäkerhets- och kriskommunikations-arbetet. Det underlättar verksamhetens kommunikation i ett skarpt läge om det redan i planer eller annan dokumentation framgår vilka personer, funktioner och grupper som har ett intresse eller är beroende av en viss information och vilka kanaler som kan användas för att nå dem.

4.4 Omvärldsbevakning

Omvärldsbevakning skapar en medvetenhet om externa hotbilder och händelser som kan påverka skyddet av information. Informationssäkerhetsteamet genomför löpande kommunövergripande omvärldsbevakning. Relevant omvärldsinformation delas med berörda och tillförs kommunens risk- och sårbarhetsanalys. En viss omvärldsbevakning behöver även göras verksamhetsnära. Hot eller händelser som förändrar informationsklassning och riskbedömningar eller påverkar skyddsbehovet behöver följas upp av verksamheten för att verifiera att informationen fortfarande har rätt skydd.

4.5 Kompetensutveckling

Beslutsfattare, chefer och medarbetare förväntas ha den kompetens som rollen kräver för att säkerställa informationssäkerheten inom den egna verksamheten och funktionen. I de fall en person ska hantera skyddsvärd, känslig eller säkerhetskänslig information bör denne erbjudas en ändamålsenlig säkerhetsutbildning i informationssäkerhet och dataskydd.

4.6 Lokala styrdokument, planer och rutiner

Även om styrdokument, handlingsplaner och rutiner tas fram gemensamt för hela kommunen behövs oftast kompletterande planer, rutiner, etc. för den egna verksamheten. Vilka de är och var de ska sparas bestäms lokalt.

5 Roller och ansvar

Roller och ansvar är tilldelade utifrån kommunens behov av struktur för informationssäkerhetsarbetet. Informationssäkerhet är kopplat till verksamhetsansvaret i alla led. Det betyder att varje nämnd eller bolagsstyrelse och varje chef som är ansvarig för en verksamhet också är ansvarig för informationssäkerheten i denna. Ytterst ligger ansvaret för informationssäkerhet på kommunstyrelsen medan ansvaret för dataskydd ligger på respektive nämnd.

5.1 Ansvarsuppdelning inom förvaltningen

- **Kommundirektör** har det övergripande ansvaret för informationssäkerhetsarbetet.
- **Stabschef** har övergripande ansvaret för dataskyddsarbetet.
- **Chefer på kontors-, verksamhets- och enhetsnivå** är samtliga informationsägare med ansvar för att den egna verksamhetens information är riktig, tillförlitlig och hanteras på rätt sätt.
- **Kontaktpersoner för dataskydd** är personer som utsetts för att tillsammans med dataskyddssamordnaren säkerställa en säker hantering och ett ändamålsenligt skydd av personuppgifter genom hela dess livscykel.
- **Dataskyddsombud** har i uppdrag att ge stöd och rådgivning till kommunens tjänstepersoner i GDPR-frågor samt att stötta det interna dataskyddsarbetet då viktiga dataskyddsfrågor behandlas.
- **Systemägare** är chefer som ansvarar för budget, avtal och att säkerhetsåtgärder i informationssystem införs, förvaltas, följs upp och utvärderas.
- **Systemförvaltare** är ett operativt stöd till system- och informationsägare.
- **Informationssäkerhetsteamet** är en sammansatt grupp med personer med expertkunskaper inom områdena informationssäkerhet, cybersäkerhet och dataskydd vars huvuduppgift är att stödja chefer, systemägare, informationsägare och medarbetare i det systematiska informationssäkerhetsarbetet i linje med styrdokument.
- **Personuppgiftsansvariga** är kommunens politiska organ, dvs. nämnderna. Respektive nämnd är ansvarig för sin egen verksamhet och för att personuppgifter behandlas enligt GDPR.
- **Personuppgiftsbiträden** är de som behandlar personuppgifter för den personuppgiftsansvarigas räkning. För parterna ska det alltid finnas ett PUB-avtal.
- **Säkerhetsskyddschefen** ansvarar för att hantera information i säkerhetsskyddsklass.
- **Alla som arbetar inom och för kommunen** har en skyldighet att hålla sig uppdaterade om vad som gäller för säker hantering av kommunens informationstillgångar och personuppgifter. I det ingår att bidra till en god informationssäkerhet genom att följa rutiner och anvisningar för säker informationshantering, utveckla kompetens och säkerhetsmedvetande genom att gå anvisade utbildningar, vara uppmärksam och anmäla olika säkerhetshändelser. Om något är oklart, fråga närmaste chef eller informationssäkerhetsteamet om råd.
- Samordnare för dataskydd och samordnare för informationssäkerhet har båda särskilda uppdrag inom ramen informationssäkerhet där:
  Dataskyddssamordnaren ansvarar för att bevaka och samordna arbetet med dataskydd och säkerställa en säker hantering av personuppgifter. Detta i linje med kommunens ledningssystem, externa krav och GDPR. I rollen ingår att samarbeta med kontaktpersoner för dataskydd, ge stöd till kommunens chefer och verksamheter samt att hålla kontakt med dataskyddsombudet – och Integritetsskyddsmyndigheten (IMY) vid behov.

Informationssäkerhetssamordnare har ansvaret att utveckla, stödja och samordna kommunens informationssäkerhetsarbete i linje med kommunens ledningssystem och externa krav. I rollen ingår att samordna informationssäkerhetsteamet, samarbeta med och ge stöd och vägledning till informationsägare, kommunens chefer och verksamheter. I rollen ingår att föreslå sådana rutiner som informationssäkerhetssamordnare ser behov av. Innehållet i sådana rutiner beslutas av, beroende av innehåll, antingen av kommundirektör, stabschef eller verksamhetschef för digitalisering och projektledning.

6 Kartläggning, klassificering (klassning) och riskarbete[7]

En säker användning och effektiv hantering av information är en förutsättning för kommunens verksamhet och för medborgarnas tilltro till kommunens förmåga att leverera en god service. För att säkerställa ett ändamålsenligt skydd behöver information och flöden bedömas och hanteras enligt stödanvisningar för kartläggning, klassning och riskhantering.

6.1 Kartläggning av information

Kartläggningar av information som kommunens verksamheter behandlar, använder och hanterar behöver genomföras årligen eller oftare vid behov, t.ex. vid större förändringar eller då nya risker identifieras. I dokumentationen bör det framgå vilka legala krav som styr informationshanteringen. Redan vid kartläggningen är det bra att fråga sig vad som skulle hända om någon obehörig kommer åt informationen, om den manipuleras eller inte går att nå. Se *Stödanvisning för kartläggning av information*.

6.2 Klassning av information

All information behöver klassas med utgångspunkt i aspekterna konfidentialitet, riktighet och tillgänglighet (KRT) enligt *Stödanvisning för klassning av information*. Klassningen utgör underlag för kunskapsuppbyggnad och kravställning på hur informationen ska hanteras, behandlas och skyddas. Notera att hållbarheten för en klassning är kortvarig. Information är föränderlig och det kan tillkomma ny information av känslig karaktär. Förutsättningarna kan även påverkas av organisationsförändringar, upphandlingar, byte av ett verksamhetssystem, införande av ny teknik, som AI eller ”Internet of things” (IoT) eller förändrade arbetssätt som kommer med nya e-tjänster. Informationsklassningen behöver därför följas upp årligen.

Vid klassningen bedöms informationens värde utifrån:

- Den funktion och betydelse den har för verksamheten.
- De konsekvenser det medför för verksamheten om informationen skulle förändras av obehörig, försvinna eller komma i orätta händer.
- Hur känslig den är för den enskildes personliga integritet.

Alla bedömningar behöver dokumenteras för att stödja det kollektiva minnet, undvika personberoende och underlätta uppföljningsarbete. Det är viktigt att det framgår:

- om informationen bedöms som verksamhetskritisk och/eller samhällsviktig.
- vilka uppgifter som bedöms som känsliga och har ett högt skyddsvärde

[7] Det är viktigt att dokumentera resultatet. Kommunen använder DirSys verktyg Security och Integrity för detta.

- vilka motiveringar som föranlett klassningsbedömningarna
- när klassningen är gjord och av vem/vilka
- – och att informationsägaren finns namngiven.

För information med ett högt skyddsvärde är även spårbarheten viktig, dvs. att i efterhand kunna härleda specifika aktivister och händelser till ett identifierat objekt eller användare.

6.3 Klassning av system

Alla digitaliserings- och IT-lösningar, tjänster och verksamhetssystem som används behöver klassas för att fastställa vilken nivå av information som kan hanteras där. Detta för att informationsägare ska kunna känna sig trygga med att de system de använder/vill använda verkligen uppfyller de krav som den informationsklassningen ställer. Systemklassning fastställs genom i förväg beslutade gränsdragningar om de säkerhetsåtgärder som anses nödvändiga för olika skyddsnivåer. En genomgång enligt *Stödanvisning för systemklassning* fastställer systemets högsta skyddsvärde. Det styr sedan vilken typ av information som kan/får hanteras i systemet. Även risker som faller utanför kravställningar i ISO 27002 ska beaktas.

På samma sätt som informationsägare behöver informera om hur informationen klassats har systemägare och leverantörer en skyldighet att informera om vilken informationsklass deras system och tjänster klarar att hantera. I de fall tjänsten inte motsvarar verksamheternas krav på säkerhet ska informationen hanteras på annat säkert sätt fram till dess att kraven är uppfyllda. Om en situation uppstår där något behöver utvecklas eller uppgraderas för att klara K2- eller K3-information bör kostnads- och tidsaspekter klargöras innan beslut tas.

6.4 Riskarbete

Den som ansvarar för en verksamhet behöver se till att informationssäkerhetsrisker analyseras, bedöms, hanteras och följs upp enligt den riskhanteringsprocess som finns beskriven i *Stödanvisning för riskhantering*. Riskarbetet görs för att begränsa och förebygga risker så att verksamheten med rimlig säkerhet kan fullgöra sina uppgifter och nå uppsatta mål. Det är även ett sätt att förebygga IT-attacker, bedrägerier och andra oegentligheter.

Riskanalysen är central, där identifieras och värderas risker. I analysen fokuserar man på sannolika händelser med konsekvens för KRT. Med ledning av riskanalysen görs sedan en bedömning av vilka åtgärder som behöver vidtas om risken inte accepteras. Åtgärder tilldelas alltid en ”riskåtgärdsansvarig” som ser till att åtgärden blir genomförd och återrapporterad. Riskanalyser ska följas upp och uppdateras minimum årligen och vid större förändringar.

Riskbedömningar inkluderar all informationshantering och alla IT-tjänster och system som används. Ett högt riskvärde följs av åtgärder som kan upprätthålla rätt skyddsnivå för informationen. Risker som inte kan undvikas, överföras eller accepteras behöver minskas så att antingen sannolikheten eller konsekvensen reduceras till nivåer som gör risken tolerabel.

Konsekvenskategorier att beakta: ekonomisk förlust, verksamhetsavbrott, överträdelse eller bristande lagefterlevnad, personskada, skada för miljö- och hälsa, negativ påverkan på kommunen (t.ex. minskat förtroende), skada på annan organisation eller samhället i stort.

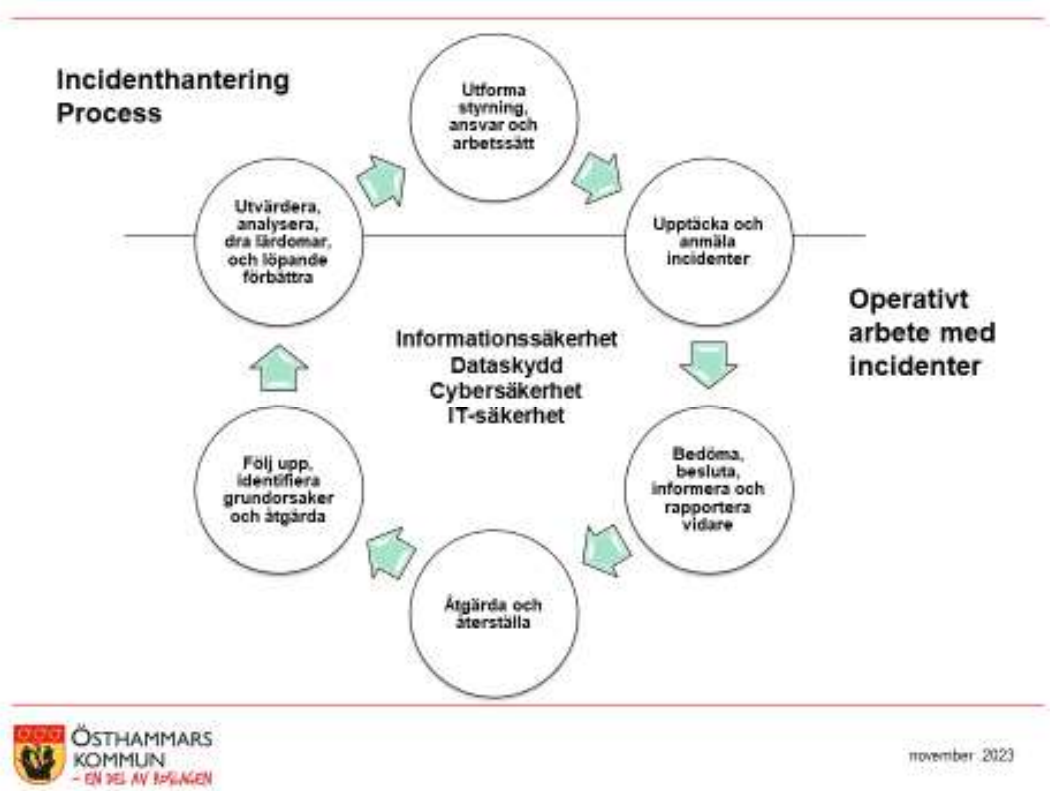
Riskacceptans: Acceptans av risker med högt riskvärde, allvarliga skadekonsekvenser och kostsamma skyddsåtgärder bör beslutas av ansvarig nämnd eller kommunstyrelsen (om flera verksamheter berörs). Beslut kan även delegeras till kontorschef. Chefer kan acceptera risker inom ramen för den egna verksamheten. Riskacceptans ska dokumenteras.

7 Incident- och kontinuitetshantering

Kommunens chefer har en nyckelroll i incident- och kontinuitetsplaneringen och även i hanteringen av olika händelser. Informationssäkerhetsteamet ger tillsammans med Säkerhetsskydd och beredskap stöd i arbetet. En kommungemensam process för incident- och kontinuitetshantering, stödanvisningar med exempel och mallar samt en e-tjänst för anmälan av informationssäkerhets- och personuppgiftsincidenter har tagits fram för att underlätta arbetet. Fördjupad information finns i *Stödanvisning för incident- och kontinuitetshantering.*

7.1 Incidenthanteringsprocess

Illustrationen nedan beskriver kommunens process för att hantera och anmäla säkerhetsincidenter relaterade till informationssäkerhet och dataskydd. I *Stödanvisning för incident- och kontinuitetshantering* beskrivs varje steg i ett eget kapitel.



7.1 Incidenthantering

Kommunens verksamheter behöver ha en beredskap för att hantera incidenter kopplade till informationssäkerhet. Detta för att i alla led skydda information, minimera avbrott i verksamheten och möjliggöra extern anmälan.

7.2 Olika typer av säkerhetsincidenter

En säkerhetsincident kan vara en eller flera händelser med negativ påverkan på informationssäkerheten, det kan även vara en kombination av olika typer av säkerhetsincidenter, t.ex. en personuppgiftsincident[8], informationssäkerhetsincident[9] och en IT-säkerhetsincident[10].

7.3 Incidentrapportering

Alla användare, anställda och leverantörer har en skyldighet att anmäla säkerhetsincidenter som påverkar eller riskerar att påverka informationssäkerheten på ett negativt sätt. Detta för att i ett tidigt skede kunna upptäcka olika händelser, undvika och lindra konsekvenserna av incidenter och minimera avbrott i kommunens verksamheter.
Det är viktigt att redan inledningsvis klara ut vilken typ av säkerhetsincident det är och vad som har orsakat problemet. Detta för att rätt personer/funktioner snabbt ska kunna vidta åtgärder som lindrar konsekvenserna av det inträffade. En del incidenter behöver även skyndsamt rapporteras vidare till myndigheter, parallellt med att berörda informeras.

I *Stödanvisning för incident- och kontinuitetshantering* beskrivs vilken säkerhetsincident som ska rapporteras var, på vilket sätt, inom vilken tid och vem som har mandat att göra det. Bedömningar och beslut som rör säkerhetsincidenter behöver dokumenteras för framtida referens, verifiering och uppföljning. Det underlättar även lärandet av inträffade incidenter, minskar risken för att en liknande händelse ska inträffa igen och förbättrar löpande informationssäkerheten då nya eller förfinade säkerhetsåtgärder införs.

7.4 Kontinuitetshantering

Vid allvarliga incidenter med stor påverkan på kommunens kritiska och samhällsviktiga verksamheter är det viktigt att ha genomarbetade kontinuitetsplaner till hands att arbeta efter. De kontinuitetsplaner som respektive verksamhet har arbetat fram i planeringsfasen kan nu komma att användas i skarpt läge.

8 Krav på säkerhetsåtgärder

8.1 Säkerhetsåtgärder kan vara

- Organisatoriska; t.ex. tydliga roller och ansvar. Rutiner, handlings- och kontinuitetsplaner samt utbildningsinsatser är andra exempel på organisatoriska, administrativa åtgärder.

[8] En **personuppgiftsincident** är en händelse som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Den kan också leda till obehörigt röjande av eller obehörig åtkomst till personuppgifter.
[9] En **informationssäkerhetsincident** är en enskild eller flera oönskade eller oväntade händelser som har - eller riskerar att få - negativa konsekvenser för verksamheten och dess informationssäkerhet.
[10] En **IT-säkerhetsincident** berör vår IT-miljö. Ofta krävs någon form av omedelbar åtgärd för att hantera en situation, t.ex. IT-haveri, problem med datorer i nätverket, virusskydd eller säkerhetsuppdateringar.

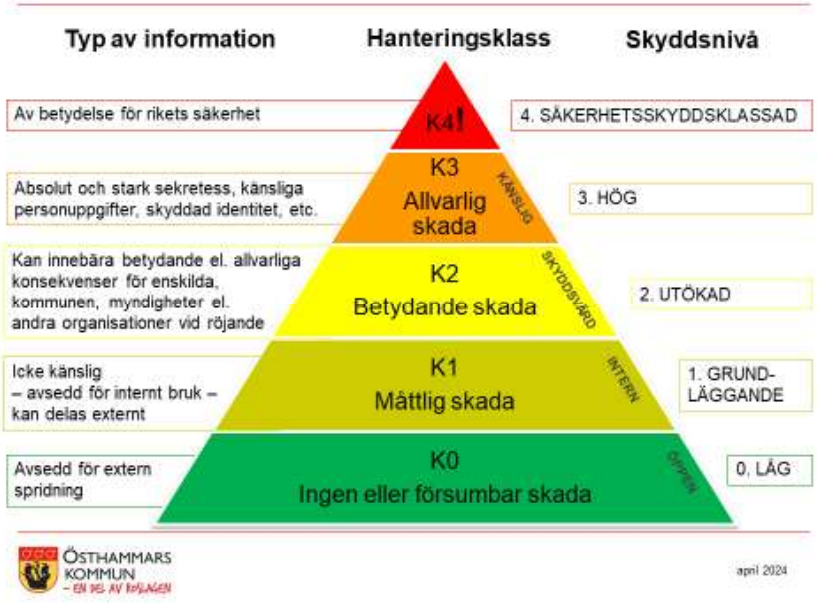
- Personrelaterade; t.ex. rutiner och processer för behörighetsstyrning när medarbetare börjar, slutar eller byter tjänst samt disciplinära åtgärder för om någon avsiktligt bryter mot styrdokumenten för informationssäkerhet.
- Fysiska; t.ex. lås och larm som skyddar information/system mot obehörig fysisk åtkomst.
- Tekniska; ändamålsenliga IT-lösningar som kan skydda information, t.ex. antivirus, säkerhetskopiering, behörighetssystem och loggning.

8.2 Öppen, intern, skyddsvärd och känslig information

Den information kommunen hanterar är i grunden öppen. Kommunen ska vara transparant och i det ingår en skyldighet att lämna ut information och handlingar när allmänheten, massmedia eller andra efterfrågar dem. Handlingsoffentligheten är ett uttryck för offentlighetsprincipen, vilken regleras i tryckfrihetsförordningen. Tanken är att insyn och öppenhet ska öka rättssäkerheten och effektiviteten i myndigheternas arbete, förhindra rättsövergrepp mot enskilda, motverka korruption och stärka allmänhetens förtroende.

Det finns också bestämmelser om sekretess i offentlighets- och sekretesslagen som begränsar rätten att ta del av allmänna handlingar. Vidare har kommunen en skyldighet att se till att känslig och skyddsvärd information hanteras på ett säkert sätt och ges ett ändamålsenligt skydd. Det gäller t.ex. känsliga personuppgifter och uppgifter av säkerhetskänslig karaktär, som aggregerad information om risker och sårbarheter och uppgifter om kritisk infrastruktur.

Verksamheternas informationsklassning ger beslutsunderlag för skyddet av information.



Triangeln illustrerar olika informationstyper, hanteringsklasser och skyddsnivåer.
K står för konfidentialitet.
Med varje skyddsnivå följer olika säkerhetskrav och skyddsåtgärder.

8.1 Säker informationshantering, kommunikation och lagring

För information klassad på K2- och K3-nivå ställs särskilda krav på säker hantering. Skyddsvärda och känsliga uppgifter behöver hanteras på ett säkert sätt genom hela sin livscykel. Det innebär att denna information endast får lagras, delas och skickas krypterad via säkra kanaler, med kommunens utrustning och behörighetsstyrning. Kollegor kan använda en gemensam kommundator, men då med sin egen inloggning.

Privat utrustning[11] *bör inte* användas för hantering av kommunens information. För behandling av skyddsvärd och känslig information *får inte* privat utrustning användas. Vid användning av mobil utrustning gäller det att vara försiktig så att verksamhetsinformation *inte* äventyras. Var och en som använder mobila enheter i tjänst behöver försäkra sig om att informationen skyddas för insyn och otillåten användning. Att inte låna ut mobil utrustning, att stänga av när den inte används och att låsa skärmar i pauser är ett minimumkrav.

Kommunen tillhandahåller krypteringslösningar och tjänster som t.ex. säker e-post och säkra videomöten som ska användas för säker kommunikation då fysiska möten inte är ett alternativ. Se *Stödanvisning för säker kommunikation och lagring* för mer information. För att utbyta känslig och skyddsvärd information mellan kommuner, regioner och statliga myndigheter kommer säker digital kommunikation användas fr.o.m. 2025 (SKR:s handslag).

Som informationsägare är det viktigt att säkerställa att de verksamhetssystem och IT-tjänster som används, utvecklas eller köps in verkligen har det skydd som behövs för att hantera K2- och K3-klassad information. Det görs bäst i dialog med systemägare och leverantörer som har en skyldighet att informera om vilken informationsklass de har kapacitet att hantera.

8.2 Distansarbete

Distansarbete avser alla former av arbete utanför kommunens lokaler och skalskydd. Information som hanteras på annan plats ska skyddas enligt samma säkerhetsskyddsnivå som om arbetet utfördes i kommunens lokaler. All distansuppkoppling till IT-miljöer som är anslutna till kommuns nätverk ska ske genom den lösning som IT-centrum tillhandahåller. Vid arbete utanför arbetsplatsen, sträva alltid efter att hitta en plats där det går att arbeta ostört, där ingen kan höra vad som sägs eller ta del av information på skärmen.

I de fall information klassad på K2- eller K3-nivå hanteras bör chefen göra en individuell bedömning om det är lämpligt att medarbetare arbetar på annan plats. Den skyddsnivå som informationsklassningen resulterat i ska alltid upprättas. Se lokala rutiner för hur t.ex. dokument med skyddsvärt och känsligt innehåll ska tas undan, låsas in och förstöras.

8.3 Identitet och åtkomst

Styrning av identitet och åtkomst är viktigt i informationssäkerhetsarbetet. Användare, tjänster, uppkopplade ”saker” (s.k. IoT, Internet of things), t.ex. sensorer, robotar eller apparater och även Artificiell Intelligens (AI) ska ges tillgång till den information och de funktioner de behöver för att utföra sitt arbete på ett lämpligt sätt. Informationsklassningen sätter ramarna för hur åtkomst ska tilldelas och hanteras för olika nivåer av information och funktioner. Hänsyn ska alltid tas till informationens skyddsvärde och individers integritet.

Åtkomst till skyddsvärd och känslig information ska ges restriktivt. Det innebär att åtkomsten behöver ges enligt klart definierade principer, tydligt ansvar och enhetliga metoder så att kontroll och säkerhet kan upprätthållas. Särskild uppmärksamhet behöver ägnas åt höga behörigheter och då användare slutar eller byter tjänst. Informationsägare behöver godkänna

[11] Med privat utrustning menas datorer, surfplattor och smarta mobiltelefoner (inte bildskärmar, hörlurar, etc.)

tilldelning och avbeställa åtkomst till information - systemförvaltare kan utföra uppgiften. För att styra åtkomst till information och tjänster i kommunens IT-miljö används tre komponenter:

- Användarens identitet, exempelvis användarnamn
- Kontroll av uppgiven identitet, så kallad autentisering
- Behörighet

En användares identitet och autentiseringen utgör en kontroll av att användaren är den som den utger sig för att vara. Kontrollen behöver utföras oavsett om det är en person eller en tjänst/”sak” som söker åtkomst till information och tjänster. Kontrollen av identiteten är grundläggande för kommunens förmåga att förhindra obehörig åtkomst, digitalisera på ett säkert sätt och för att det ska gå att förlita sig på loggar.

Krav på behörighet kopplad till kommunens klassningsmodell
Lagstiftning och informationsklassning styr vilken bevisstyrka som ska användas för identitetskontroll. Den kontroll som ger starkast bevisföring är stark autentisering. Det innebär att verksamheten behöver kontrollera användarens identitet mot en viss identitetshandling, exempelvis pass, innan behörigheten lämnas ut till användaren. Här behövs tydliga säkerhetsrutiner och beslutsfattande av chef. Användaren ska sedan använda s.k. multifaktorkontroll, t.ex. ett lösenord och bank-id för att få åtkomst till informationen.

För öppen information ställs inga krav på identitet eller autentisering. För K1-klassad information kan användarnamn och lösenord användas. För K2-klassad information gäller tillämpning av multifaktorskontroll (MFA) eller krypteringslösning. För K3-klassad information ska stark autentisering alltid tillämpas. I *Stödanvisning för identitet och åtkomst* ges anvisningar för hur identiteter och åtkomst ska hanteras. Vid påbörjad, förändrad och avslutad anställning gäller HR:s ”onboarding-offboarding-process”.

8.4 Loggning och spårbarhet

Det ska vara möjligt att följa upp aktiviteter i kommunens informationshantering där lagstiftning och informationsklassning så kräver. Detta gäller för all hantering av kommunens känsliga och skyddsvärda information, oavsett var eller i vilken form hanteringen sker och om den sker manuellt eller digitalt. Detta inkluderar inpasseringsutrustning, larm, IoT och liknande lösningar. Målet med loggning och spårbarhet är att upprätthålla kontrollen och säkerheten hos information som hanteras och överförs internt eller externt. Bestämmelser om loggning, bevarande och gallring av loggar ska följa gällande dataskyddslagstiftning.

Informationsägaren bestämmer genom att klassa information vilka verksamhetskrav som ska ställas på spårbarhet och loggning. Även logginformationen ska ha skydd mot obehörig åtkomst och manipulation. Den personliga integriteten ska alltid värnas i tekniska och organisatoriska åtgärder för spårbarhet, återskapande av information och uppföljning av händelser. Om det inte är nödvändigt för syftet ska personuppgifter *inte* ingå i loggen. Vid informationsflöden inom och mellan system och tjänster ska det gå att följa hur information överförts. När en verksamhet beställer, får ta del av och granskar loggar ska det ske enligt kontrollerade former i samråd med kontorschef, informations- eller systemägare. Se *Stödanvisning för loggning och spårbarhet* för mer information.

8.5 Anskaffning och utveckling

I de fall då chefer, nämnder och bolag uppdrar åt andra att hantera verksamhetens information ska avtalet omfatta sådana krav att informationen hanteras, skyddas och följs upp i enlighet med kommunens styrdokument samt verksamheternas krav på säkerhet och skydd utifrån klassning. I *Stödanvisning för anskaffning och utveckling* beskrivs hur.

Informationssäkerhetskrav ska alltid beaktas i ett tidigt skede, såväl vid upphandling som vid utveckling, digitalisering och satsningar på ny teknik. Vidare ska informationssäkerhetskrav ingå vid upprättande av avtal och överenskommelser. När kommunen köper IT-tjänster av extern part eller förlägger drift av system och tjänster externt ska det redan vid upphandling säkerställas att skyddsnivån svarar mot klassningen av den information som ska hanteras där. En riskbedömning ska alltid genomföras innan avtal ingås. Även vid ändring av leverantörers tjänster eller avtal ska en förnyad riskbedömning genomföras. För information som bedöms som skyddsvärd och känslig samt för verksamhetskritiska och/eller samhällsviktiga tjänsteleveranser ska kommunen regelbundet kunna övervaka, granska och genomföra revision.

Leverantörer av IT-tjänster ska uppdras att klassa sina system och tjänster, och skriftligen deklarera hur väl de svarar mot definierade informationssäkerhetskrav. Detta för att ge informationsägarna ett underlag för bedömning av vilken nivå av informationsklass som kan hanteras där. Vidare ska leverantörer säkerställa att säkerhetsåtgärderna motsvarar skyddsbehovet för den information som redan finns i tjänsten och att en skyndsam avvikelse- och incidentrapportering görs när informationssäkerheten påverkas eller riskerar att påverkas. Leverantörer som kan få tillgång till eller ska använda, behandla eller hantera känslig och skyddsvärd information behöver skriva under kommunens sekretessavtal. I de fall det gäller personuppgifter ska det finnas PUB-avtal mellan kommunen och organisationen. Det ska finnas möjlighet för kommunen att genomföra en årlig kontroll i syfte att säkerställa att leverantörens informationssäkerhet fortfarande är intakt.

8.1 Drift och förvaltning av IT-tjänster

IT-drift ska säkerställa att verksamhetens IT-tjänster fungerar smidigt och effektivt. Det omfattar bl.a. rutinmässiga uppgifter som systemövervakning, nätverksadministration, hantering av servrar, applikationsuppgraderingar, säkerhetspatchning och incidenthantering. Driftleverantören ska säkerställa att alla väsentliga delar av IT-miljön svarar mot de informationssäkerhetskrav som är överenskommet enligt avtal och att verksamheterna informeras om förändringar och händelser som påverkar/riskerar att påverka informationssäkerheten. Målet är att säkerställa hög tillgänglighet, prestanda och säkerhet för IT-tjänsterna samt att skydda verksamhetens information enligt klassning. Driftförvaltarens ansvar regleras i ett serviceavtal som tecknats med driftleverantören, oavsett om det är IT-centrum eller en extern driftleverantör. Dokumenterade rutiner för IT-tjänsters livscykelhantering ska finnas.

9 Efterlevnad

Granskning: Kommunstyrelsen granskar löpande efterlevnaden av programmet för informationssäkerhet för att upprätthålla rätt nivå av säkerhet och skydd. Interna revisioner och externa oberoende granskningar kan göras löpande och vid större förändringar.

Mätningar och ständiga förbättringar: Kommunen strävar efter ständiga förbättringar av informationssäkerheten. Förbättringarna ska mätas mot programmet för informationssäkerhet och genom årliga mätningar. Obligatoriska mätningar är MCF:s cybersäkerhetskoll och en intern mognadsmätning. Andra mätningar kan bli aktuella om behov finns.

Uppföljningar och rapportering av informationssäkerhets- och dataskyddsarbetet till KFLG ska genomföras regelbundet i linje med i kommunens ledningssystem. Innehåll i rapportering:

- Hot och förändringar i omvärlden som kan påverka informationssäkerhet/dataskydd
- Kompetens och efterlevnad av styrdokument (status och behov)
- Inträffade säkerhetsincidenter med större påverkan på verksamheten
- Resultat från genomförda mätningar, granskningar och revisioner
- Ständiga förbättringar och förslag på nya säkerhetsåtgärder
- Övriga frågor

Samordnarna ansvarar för rapportering om informationssäkerhet respektive dataskydd. Dataskyddsombudet kan vid behov ge en kompletterande årlig rapport.

Kommunstyrelsens årliga genomgång: Kommunstyrelsen ska erbjudas en årlig genomgång av informationssäkerhets- och dataskyddsarbetet. Syftet är att ge en bild av hur kommunen ligger till i förhållande till styrdokument, externa krav och interna behov samt att skapa ett kunskapsunderlag för ständiga förbättringar.

10 Stöd och kontakt

Informationssäkerhetsteamet ger och utvecklar löpande stöd till kommunens verksamheter. Mer information, styrdokument, handlingsplaner, kommungemensamma rutiner, stödanvisningar och annat stödmaterial tillgängliggörs löpande på Ines: https://ines.osthammar.se/service-support-och-stod-i-arbetet/informationssakerhet

Vill du komma i kontakt med informationssäkerhetsteamet är du välkommen att använda vår funktionsbrevlåda infosakerhet@osthammar.se eller ringa oss direkt via Teams eller telefon:

- Informationssäkerhetssamordnare Maria Langen: 0173-861 08
- Dataskyddssamordnare Håkan Åhlénius: 0173-854 12
- Anneli Lennström (biträdande informationssäkerhetssamordnare): 0173-862 43