**Administrativa enheten**
Emmy Johansson
emmy.johansson@svalov.se



# Riktlinje för informationssäkerhet

Dokumentinformation

Diarienummer: KS 231-2021:560

För revidering ansvarar: Kanslichef

För uppföljning ansvarar: Kanslichef

Dokumentansvarig: Kanslichef

Dokumentet gäller för: Alla kommunens verksamheter

Giltighetsperiod: 2025 - tillsvidare

Aktualitetsprövas/revideras: En gång per mandatperiod samt vid behov

Ersätter: Informationssäkerhetspolicy daterad 2015-08-17, i de delar som inryms i denna riktlinje.

Publicerat i kommunal författningssamling: 2025-10-16

Antaget: Kommunstyrelsen 2025-09-15, § 222

# Innehåll

Riktlinje för informationssäkerhet ..... 1
Inledning ..... 3
Begreppsdefinition ..... 3
Utgångspunkt ..... 3
Ledningssystem för informationssäkerhet ..... 3
Mål med informationssäkerhetsarbetet ..... 4
Dokumentstruktur ..... 4
Organisation, roller och ansvarsfördelning ..... 4
Övergripande principer för informationssäkerhetsarbetet ..... 6
*Riskbaserat arbetssätt ..... 6*
*Utbildning ..... 6*
*Informationstillgångar och informationsklassning ..... 6*
*Konsekvensbedömning och riskanalys ..... 6*
*Informationshanteringsplan ..... 7*
*Kontinuitetshantering ..... 7*
*Informationssäkerhetsincidenter ..... 7*
*Upphandling ..... 8*
Säkerhet ..... 8
*Personalsäkerhet ..... 8*
*Fysisk säkerhet ..... 9*
*IT-säkerhet ..... 9*
Uppföljning ..... 11

# Inledning

Kommunens informationssäkerhet omfattar alla verksamheters informationstillgångar, både information som hanteras digitalt och analogt. Detta dokument, *Riktlinje för informationssäkerhet*, konkretiserar kommunens informationssäkerhetspolicy med information om viktiga områden. Riktlinjen beskriver även vad som behöver etableras för att uppfylla informationssäkerhetspolicyn och integrera informationssäkerhetsarbetet som en naturlig del i kommunens verksamheter.

# Begreppsdefinition

**Informationssäkerhet:** Den samlade, övergripande säkerheten som ska se till att den information som finns i en organisation alltid är korrekt, tillgänglig och skyddad.

**Dataskydd:** Skydd och hantering av personuppgifter som behandlas av den personuppgiftsansvarige. Utgör en av delarna som ryms inom begreppet informationssäkerhet.

**IT-säkerhet:** Cybersäkerhet och åtgärder inom detta område som syftar till att skydda information och IT-system, både från interna och externa hot. Utgör en av delarna som ryms inom begreppet informationssäkerhet.

# Utgångspunkt

Svalövs kommuns informationssäkerhetsarbete ska i linje med rekommendationer från Myndigheten för samhällsskydd och beredskap (MSB) samt den etablerade standarden SS-ISO/IEC 27000 utgå från följande ledord:

- **Tillgänglighet.** Information ska finnas tillgänglig när den behövs och på förväntat sätt.
- **Riktighet.** Vår information ska vara korrekt och tillförlitlig. Informationen ska skyddas mot oönskad förändring och förstöring.
- **Spårbarhet.** Aktiviteter ska kunna härledas i efterhand. Vi ska kunna visa vad som har hänt och vem som har gjort vad i våra system.
- **Konfidentialitet.** Vår information ska inte göras tillgänglig eller avslöjas för obehöriga.

Utöver dessa ledord ska informationssäkerhetsarbetet även bedrivas utifrån gällande lagstiftning så som dataskyddsförordningen (GDPR), NIS-direktiv samt sektorsspecifika lagar och förordningar för respektive nämnd.

# Ledningssystem för informationssäkerhet

Ett ledningssystem för informationssäkerhet (LIS) är ett stöd för hur informationssäkerhetsarbetet styrs i olika verksamheter. Ett LIS är en organisations olika processer för styrning och ledning av informationssäkerhetsarbetet. Genom att ha ett LIS finns grunden för ett systematiskt informationssäkerhetsarbete i form av styrdokument och processer. Dessa styrdokument och processer behöver vara kända av kommunens medarbetare och följas upp regelbundet.

För att realisera ett ledningssystem för informationssäkerhet inom Svalövs kommun behöver det finnas styrdokument och processer för kommunens informationssäkerhetsarbete. *Informationssäkerhetspolicy* och *Riktlinje för informationssäkerhet* utgör den kommunövergripande grunden för hur arbetet med informationssäkerhet bör bedrivas. Utifrån dessa styrdokument kan i sin tur övergripande samt verksamhetsspecifika riktlinjer, rutiner, processbeskrivningar, instruktioner och metodstöd tas fram. Alla dessa delar kommer tillsammans utgöra kommunens LIS och fungera som ett stöd i det dagliga arbetet med informationssäkerhet.

# Mål med informationssäkerhetsarbetet

Målet med Svalövs kommuns informationssäkerhetsarbete är, som framgår av policyn, följande:

- Att informationen hos respektive verksamhet ska hanteras korrekt i det dagliga arbetet och vid störningar av olika slag.
- Att Svalövs kommuns informationshantering ska vara tillräckligt säker, effektiv och skyddad utifrån den typ av information som avses.
- Att Svalövs kommun ska bedriva ett strukturerat och systematiskt informationssäkerhetsarbete utifrån gällande policy, riktlinjer och rutiner samt att arbetet ska följas upp årligen.

# Dokumentstruktur

**Informationssäkerhetspolicy**: kommunövergripande styrdokument som utgör grunden för arbetet med att skydda och säkerställa kommunens informationstillgångar.

**Riktlinje för informationssäkerhet:** kommunövergripande riktlinje som utgår från informationssäkerhetspolicyn och konkretiserar policyn genom att övergripande beskriva hur kommunen bör arbeta med informationssäkerhet.

**Vägledning inom olika områden*:*** kommunövergripande vägledningar som utifrån policy och riktlinje ännu mer konkretiserar rekommenderade arbetssätt inom olika områden.

**Sektorsspecifik rutin:** konkret beskrivning av ett i förväg bestämt arbetssätt som respektive nämnd tar fram vid behov. Ska utgå från policy, riktlinje och vägledning.

# Organisation, roller och ansvarsfördelning

För att arbetet med informationssäkerhet ska kunna bedrivas strukturerat och systematiskt ska det inom varje förvaltning finnas en organisation som hanterar frågor om informationssäkerhet inklusive dataskydd. Nedan följer det ansvar som olika roller har gällande kommunens informationssäkerhetsarbete.

**Verksamhetsansvar**: Ansvaret för informationssäkerhet följer verksamhetsansvaret i form av delegationsordning. Ansvarig för en viss nämnd, verksamhet, avdelning och enhet ansvarar för informationssäkerheten inom sitt område. Detta innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Detta innebär

att se till att relevanta styrdokument tas fram, att medarbetare utbildas och att arbetet följs upp systematiskt.

**Sektorschef:** Ansvarar för att det finns ett systematiskt arbete med informationssäkerhet inom sektorn. Ansvarar för att sektorsspecifika riktlinjer, rutiner och instruktioner tas fram, implementeras och följs upp. Ansvarar för årlig uppföljning av informationssäkerhetsarbetet inom sektorn.

**Verksamhets-/avdelningschef:** Ansvarar för arbetet med informationssäkerhet inom sitt område. Ansvarar för att verksamhetsspecifika styrdokument tas fram, implementeras och följs upp. Ansvarar för att enhetschefer får utbildning inom informationssäkerhet och dataskydd.

**Enhetschef:** Ansvarar för arbetet med informationssäkerhet inom sin enhet. Ansvarar för att enhetsspecifika styrdokument tas fram, implementeras och följs upp. Ansvarar för att medarbetare får utbildning inom informationssäkerhet och dataskydd.

**Medarbetare** ansvarar för att följa styrdokument och rutiner samt att rapportera upptäckta brister inom området. Ansvarar även för att gå utsedda utbildningar inom områdena informationssäkerhet och dataskydd.

**Informationsägare** ansvarar för att informationen i system och processer inom verksamhetsområdet hanteras och förvaltas på ett säkert sätt. Informationsägaren är ansvarig för att informationsklassning och riskanalyser genomförs. Varje system och process ska ha en utsedd informationsägare, om detta inte är utsett innehas denna roll av sektorschef.

**Systemägare** är huvudansvarig för verksamhetens egna informationssystem och utser systemförvaltare. Rollen bemannas som regel av sektorschef.

**Systemförvaltare** ansvarar för den dagliga driften och förvaltningen av informationssystem.

**IT-funktionen** innehar det verkställande ansvaret för kommunens IT-driftmiljö. Samverkar med informationsägare och systemägare för att uppnå adekvat nivå på säkerhetsåtgärder för system och information.

**Informationssäkerhetssamordnare** leder och samordnar kommunens informationssäkerhetsarbete, ansvarar för att ta fram förslag till kommunövergripande policy, riktlinjer, vägledningar och rutiner samt stödjer kommunens verksamheter i frågor som rör informationssäkerhet. Informationssäkerhetssamordnaren följer upp informationssäkerhetsarbetet och rapporterar till ledningen.

**Dataskyddsombudet** ska vara oberoende och självständigt. Ska informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar personuppgifter. Ska även övervaka efterlevnaden av dataskyddsförordningen.

**Dataskyddssamordnare** har en stödjande funktion och ett särskilt ansvar för att aktivt driva och utveckla arbetet med informationssäkerhet och dataskydd inom respektive nämnds verksamheter.

# Övergripande principer för informationssäkerhetsarbetet

### Riskbaserat arbetssätt

Ett systematiskt informationssäkerhetsarbete bygger på att verksamheten analyserar och arbetar med sina risker. Verksamhetens informationshantering ska ske på ett sätt som skyddar informationen på bästa sätt. Genom risk- och sårbarhetsanalyser, informationsklassningar, konsekvensbedömningar, kontinuitetshantering samt incidenthantering arbetar verksamheten med riskanalys och riskhantering på olika sätt. För att kunna arbeta med dessa områden behöver det finnas tydliga styrdokument, processer och arbetssätt. Det behöver även finnas kunskap om dessa områden inom kommunens olika verksamheter, samt en tydlig ansvarsfördelning.

### Utbildning

All personal ska genomgå grundläggande utbildning i informationssäkerhet, vid nyanställning och sedan minst en gång årligen. Utbildningen sker i första hand digitalt. Ansvarig chef ska säkerställa att samtliga medarbetare har tillgång till utbildningsportal och följa upp att utbildningar görs.

### Informationstillgångar och informationsklassning

Alla informationstillgångar ska förtecknas i respektive nämnds informationshanteringsplan. Med informationstillgångar avses till exempel informationssystem och/eller processer och dess information samt pappershandlingar eller digitala handlingar.

Informationstillgångarna ska även klassificeras (klassas). Detta innebär att på ett enhetligt sätt värdera organisationens information utifrån begreppen konfidentialitet, riktighet och tillgänglighet. Genom att klassa informationen och vilka konsekvenser ett otillräckligt skydd kan innebära har verksamheten möjlighet att ta fram åtgärder för att minska risken för konsekvenser och öka möjligheten att skydda informationen. Eftersom olika informationstyper skiljer sig åt behöver en klassning göras för att säkerställa att informationen varken har för lågt eller för högt skydd.

Klassningen görs utifrån en kommungemensam modell och ska dokumenteras. Klassningen ska följas upp årligen och uppdateras vid behov om informationen eller förutsättningarna för denna förändras.

### Konsekvensbedömning och riskanalys

En konsekvensbedömning, också kallad DPIA (Data Protection Impact Assessment), görs enligt dataskyddsförordningen i samband med att en ny behandling av personuppgifter ska genomföras som kan innebära en stor risk för den enskilde. Detta kan exempelvis bli aktuellt om personuppgifter ska behandlas i ett nytt system eller om redan tillgängliga personuppgifter ska behandlas på ett annat sätt än förut.

En DPIA är i grunden en riskanalys som görs för att identifiera de risker som finns kopplat till den personuppgiftsbehandling som görs. Även vid tillfällen då det inte rör sig om personuppgifter kan kommunens verksamheter hantera känslig information där behandlingen av den på samma sätt behöver riskbedömas. Genom att identifiera de risker som kan finnas med hanteringen av informationen kan åtgärder tas fram för att minska riskerna. På så sätt ökar möjligheterna att skydda informationen.

Sektorschef ansvarar för att riskanalys blir gjord vid behov samt godkänner framtagna åtgärder. Sektorschef ansvarar för att riskanalysen följs upp årligen och vid behov.

### Informationshanteringsplan

Varje nämnd ansvarar för att ha en informationshanteringsplan som beskriver hantering, arkivering och gallring av allmänna handlingar. Genom att ha en sådan plan blir det tydligt hur verksamheten ska hantera sin information för att säkerställa att likvärdig information hanteras på samma sätt oavsett vem i verksamheten som hanterar den. Genom att följa informationshanteringsplanen säkerställs att information hålls tillgänglig och skyddad på det sätt som blivit beslutat.

Bestämmelser om informationshanteringsplan finns i arkivreglementet. Informationshanteringsplanen ska aktivt förvaltas och revideras vid behov. Sektorschef ansvarar för att uppföljning och att eventuell revidering görs.

### Kontinuitetshantering

Kommuner behöver inom sitt arbete med krisberedskap fastställa hur länge avbrott i åtkomst till verksamhetssystem är acceptabla, alltså hur länge verksamheten kan bedrivas utan stora svårigheter vid avbrott. För att kunna fastställa detta behöver en kontinuitetsplan upprättas. I en kontinuitetsplan ska det framgå hur olika aktiviteter inom en verksamhet ska kunna fortlöpa vid någon typ av störning.

Eftersom en kontinuitetsplan innehåller information om verksamheten och dess reservrutiner i ett utsatt läge behöver denna plan skyddas på rätt sätt. Det behöver även finnas rutiner för att hålla informationen i planen och dess reservrutiner uppdaterad och aktuell för att den ska gå att förlita sig på i skarpt läge.

Kontinuitetsplanen behöver även vara en integrerad del av den löpande verksamheten och systematiskt uppdateras, revideras och övas. Genom att ha en fungerande kontinuitetshantering ökar möjligheten för verksamheter att klara av störningar och fortsätta bedriva sitt arbete. Varje nämnd är ansvarig för att bedriva sitt arbete med krisberedskap, och varje sektorschef ansvarar för att en kontinuitetsplan för verksamheten tas fram.

Om en verksamhet har tagit fram en kontinuitetsplan som involverar en annan verksamhet eller avdelning behöver detta samordnas. Genom att samordna kan berörda parter få en samsyn kring prioriteringar och eventuella hinder som kräver en annan lösning. Genom att lyfta dessa frågor minskar risken för att ett beroende av en annan verksamhet inte kommer fungera i praktiken.

### Informationssäkerhetsincidenter

Informationssäkerhetsincidenter är händelser där information på något sätt har riskerats. Det kan exempelvis vara personuppgiftsincidenter, avvikelser för enskild eller IT-incidenter. Rapportering, utredning och hantering av incidenter ska ske enligt de etablerade rutiner för rapportering som finns i kommunens verksamheter.

Att rapportera en incident betyder att en händelse (inte en person) rapporteras och är en viktig del av kvalitets- och förbättringsarbetet inom kommunen. Genom att rapportera händelser där hanteringen av information inte varit säker kan riskerna analyseras och åtgärdas för att göra hanteringen säkrare framöver.

För att incidentrapportering ska bli en naturlig del i det dagliga arbetet behöver det finnas en kunskap i kommunens verksamheter om vad som räknas som en incident och hur processen för rapportering och hantering ser ut. Det behöver även finnas en förståelse för att det är händelsen som ska rapporteras och att detta är ett led i verksamhetens förbättringsarbete. Det är viktigt att verksamheten ser till händelsen och inte personen för att minska risken för att en enskild utses till syndabock vid en rapporterad incident.

### Upphandling

Vid upphandling är det viktigt att ta med krav gällande informationssäkerhet och dataskydd från början. Genom att göra en riskanalys/konsekvensbedömning i ett tidigt skede tydliggörs vilka krav kommunen bör ställa på leverantören redan inför upphandlingen. Informationssäkerhetskraven bör utgå från områdena *Tillgänglighet, Riktighet, Spårbarhet och Konfidentialitet* (se stycke om utgångspunkt ovan).

Genom att vara noga med riskanalysen/konsekvensbedömningen redan inför en upphandling blir verksamheten medveten om vilka risker som finns med det system eller den tjänst som ska upphandlas. På så sätt kan åtgärder för att motverka dessa risker tas med i beräkningen från början och göra att kommunens upphandlade system och tjänster är så säkra som möjligt.

Vid upphandling som faller under bestämmelser om säkerhetsskydd behöver särskilda åtgärder vidtas.

## Säkerhet

### Personalsäkerhet

Vid rekrytering bör bakgrundskontroll på den som söker anställning utföras i förhållande till vilken information personen ska ges tillgång till och vilka risker som kan uppstå. Bakgrundskontroller ska utföras i enlighet med beslutade styrdokument inom kommunen.

Medarbetare ska ges tillräcklig information om sin roll och sitt ansvar för informationssäkerhet innan de får åtkomst till känslig information eller informationssystem. Detta innefattar information om:

- det egna ansvaret för att följa regelverk,
- att skydda autentiseringsinformation och information,
- att endast ta del av information som behövs för att kunna utföra sina arbetsuppgifter,
- att logguppföljning utförs, samt
- vilka påföljder som kan bli aktuella om regelverk inte efterlevs.

Det ska finnas processer för registrering och avregistrering av användare och tilldelning av behörigheter till system. Vid avslut av anställning ansvarar närmsta chef för att samla in de tekniska enheter som medarbetaren haft under sin anställning, exempelvis dator och telefon. Likaså de enheter som kan ge personen tillträde till lokaler så som tagg samt SIS- eller SITHS-kort.

Ansvarig chef ansvarar även för att behörigheter tas bort från verksamhets- och informationssystem genom att enligt gällande rutin meddela IT-avdelningen om anställningens avslut. Genom att avsluta behörigheter minskar risken för att obehörig personal har fortsatt tillgång till information efter att deras anställning upphört.

## Fysisk säkerhet

Den fysiska säkerheten skall organiseras så att verksamhetens medarbetare och uppdragstagare, lokaler, utrustning och informationstillgångar skyddas mot hot så som inbrott, stöld, brand, översvämning, olyckor och katastrofer. Dessa hot kan orsakas av exempelvis fel i tekniska system, sabotage eller av andra händelser. Kommunens lokaler ska ha erforderliga skyddsåtgärder för att hindra obehörigt tillträde. Tillträde till utrymmen där det finns informationstillgångar av känslig karaktär ska begränsas.

Programvara, utrustning, dokument eller annan lagringsmedia som innehåller känslig information ska hanteras på ett säkert sätt och som utgångspunkt inte avlägsnas från kommunens lokaler. Mobiltelefon och bärbar dator som tas med från kommunens lokaler behöver hanteras och förvaras på ett säkert sätt.

Om en dator, mobiltelefon eller annan av kommunens enheter blir stulen ska detta hanteras enligt gällande rutin och genast anmälas till polisen och till kommunens IT-avdelning. Det ska även rapporteras enligt rutin som en personuppgiftsincident eftersom det kan finnas risk för att personuppgifter som finns på dessa enheter röjs.

Utskrift ska göras på någon av kommunens skrivare och ska inte göras på skrivare hemma hos kommunens medarbetare. Utskrift ska som huvudregel göras genom privat utskrift i kommunens lokaler för att skydda dokument och handlingar från obehöriga.

Det är viktigt att låsa datorn om den lämnas utan uppsikt eftersom det minskar risken för att någon obehörig tar del av information på datorn.

## IT-säkerhet

### *Behörighet och loggning*

Åtkomst till information och system inom kommunen ska styras med hjälp av organisatoriska och tekniska skyddsåtgärder. Exempel på detta är behörighetsstyrning samt loggning och logguppföljning.

Behörigheter innebär vilken tillgång en medarbetare har till olika delar av verksamhets- och informationssystem. Behörigheter ska ges utifrån medarbetarens roll och ansvarsområden och enbart gälla för den information som är nödvändig för det dagliga arbetet. Genom att styra behörigheter minskar risken för att personal har tillgång till mer information än nödvändigt.

Loggar är ett sätt att följa den aktivitet som sker i kommunens olika verksamhets- och informationssystem. Genom att logga aktivitet i systemen så arbetar kommunen med *spårbarhet* för att kunna förebygga, upptäcka och rätta till relevanta fel, oönskade händelser och förändringar i information. Loggar ska enbart tas i den utsträckning som krävs, lagras under en bestämd tid och enbart finnas tillgänglig för de som har behörighet att ta del av dem.

### *Användaridentitet och lösenord*

Varje användare ska ha en individuell användaridentitet som är personlig och som enbart ska användas av den enskilda medarbetaren. All aktivitet i systemen loggas och kopplas till den individuella användaridentiteten, vilket innebär att varje medarbetare ansvarar för de aktiviteter som sker med den egna användaridentiteten. Det är därför viktigt att inte låna ut sin inloggning till någon annan eftersom det då inte går att säkerställa vem som har gjort vad i systemet.

Vid en loggkontroll kommer alla aktiviteter kopplas till den inloggning som har använts. På så sätt kan en medarbetare som lånat ut sin inloggning bli ansvarig för aktiviteter som någon annan har gjort. Det finns även en risk att en medarbetare som använder en kollegas inloggning plötsligt har tillgång till mer information än vad som är nödvändigt.

Ansvarig chef ansvarar för att vid behov genomföra granskning av loggar samt användarnas olika åtkomsträttigheter.

***Internet***
Internet är ett arbetsverktyg och ska användas därefter. Vid användande av Internet kan säkerheten i kommunens lokala nätverk påverkas. Användandet av Internet ska ske inom ramen för varje medarbetares uppdrag. Hemsidor med exempelvis rasistiskt, våldsinriktat eller sexuellt innehåll får som grund inte besökas. Finns det ett behov av att inom sitt uppdrag besöka sådana hemsidor behöver medarbetare informera ansvarig chef och IT-avdelning om detta. Ställningstagandet till att besöka en sådan hemsida ska även dokumenteras för att säkerställa att det finns en grund för detta.

***E-post***
E-post är ett viktigt arbetsverktyg som ska användas enligt kommunens gällande rutiner. Mejlsystemet är inget lagringssystem och har en arkiveringsfunktion som gör att e-post automatiskt arkiveras efter 180 dagar. Det är därför viktigt att spara relevanta mejl på samma sätt som övriga dokument, för att säkerställa att relevant information fortsätter att finnas tillgänglig. Personuppgifter och känslig information ska som grund inte hanteras i mejlsystemet.

***Säkerhetskopiering, skydd mot skadlig kod och hantering av tekniska sårbarheter***
Säkerhetskopior av information och programvara ska tas och testas regelbundet. Det ska finnas rutiner för säkerhetskopiering och återläsning av informationen så att informationens och IT-miljöns riktighet, tillgänglighet och avsedda funktion skyddas samt att skydd mot oönskad påverkan, ändring eller insyn säkras.

Det ska ske löpande genomsökning och analys av tekniska sårbarheter i Svalövs kommuns IT-miljö. Det ska finnas rutiner så att information om tekniska sårbarheter erhålls i tid, att sårbarheter kan analyseras och att lämpliga åtgärder kan vidtas för att behandla de risker som sårbarheter medför.

För att uppnå spårbarhet och för att göra incidentutredningar möjliga ska kommunens IT-resurser och infrastruktur övervakas och loggas i den utsträckning som krävs. Genom detta arbete kan kommunen arbeta förebyggande samt upptäcka och rätta till fel, oönskade händelser och förändringar i nätverk, IT-system eller programvara. Likaså kan IT-incidenter och hot, så som skadlig kod eller intrångsförsök, identifieras och hanteras.

För att minska risken för att skadlig kod förs över genom ett USB-minne ska dessa som grund inte användas. Om en fil behöver delas, antingen inom eller utanför organisationen, ska istället kommunens tjänst för säker fildelning användas. I denna tjänst kan en medarbetare ge andra medarbetare behörighet att se en viss fil under en viss tid. Genom att använda fildelning som sker via ett av kommunen godkänt system minskar risken att information delas genom mer osäkra system. Genom att använda säker fildelning minskar risken för att skadlig kod förs över till datorn samt att obehöriga tar del av information som

finns på USB-minnen. Om det i vissa fall finns behov av att använda USB-minne ska IT-avdelningen kontaktas.

# Uppföljning

Uppföljning av informationssäkerhetsarbetet ska ske årligen och vid behov. Varje nämnd ansvarar för uppföljningen som bör följa av verksamhetsstyrningen. Uppföljning är en viktig del av det systematiska informationssäkerhetsarbetet samt det årliga kvalitets- och förbättringsarbetet. Genom att följa upp hur arbetet med informationssäkerhet bedrivs finns möjligheten att göra justeringar i rutiner, arbetssätt eller organisation för att förbättra arbetet inom området.

Kommunstyrelsen ska återkommande få information över hur arbetet med informationssäkerhet fortlöpt under perioden. Denna återrapportering sker i samma rapport som arbetet med GDPR presenteras i. Informationssäkerhetssamordnaren ansvarar för ledningens genomgång.