Riktlinjer för informations-säkerhet inom Östhammars kommun

Antaget av	Kommunfullmäktige
Antaget	2021-11-09 § 149
Gäller för	KS, nämnder, bolag/koncernen
Dokumentansvarig	Säkerhetsskyddschef

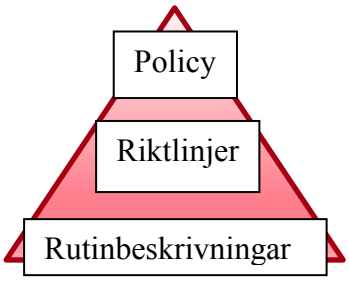
ÖSTHAMMARS KOMMUN
– EN DEL AV ROSLAGEN

Innehåll

1. Styrning

Östhammars kommuns säkerhetsskyddschef och beredskapssamordnare har det strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet. Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhetsarbete.

1.1 Styrdokument för informationssäkerhet



Policy för informationssäkerhet

Riktlinje för informationssäkerhet
Riktlinje för hemlig information

Östhammars kommuns informationssäkerhetspolicy är ett dokument som redovisar kommunens övergripande mål och inriktning med informationssäkerhet. Detta dokument – Riktlinjer för informationssäkerhet – konkretiserar informationssäkerhetspolicyn med mer detaljerad information och regler för hur information får hanteras inom kommunen.

Policyn och riktlinjen syftar också till att klarlägga roller och ansvar, vad som avses med informationssäkerhet samt övergripande krav på hur arbetet ska genomföras och följas upp.

Kraven på informationssäkerhet utgår från kommunledningens och verksamhetens krav på funktion och tillämplighet samt från gällande lagar, förordningar och föreskrifter.

Informationssäkerhet omfattar hela kommunens verksamhet och all information oavsett om den finns i datorer, i ett telefonsamtal eller på ett papper. Då stora delar av informationen hanteras med hjälp av IT-system så handlar informationssäkerhet även om teknik. För att kunna säkerställa en tillräcklig nivå av informationssäkerhet kommunens olika förvaltningar och bolag ska informationssäkerhetsarbetet bedrivs systematiskt och långsiktigt.

Det är otillåtet att upprätta avtal och överenskommelser som åsidosätter riktlinjen för informationssäkerhet. Riktlinjen, är liksom policyn, obligatoriska styrdokument som ska samtliga verksamheter inom kommunen ska efterleva. Policyn och riktlinjen för informationssäkerhet är fastställd av Kommunfullmäktige. De gäller fr.o.m. 2021-00-00.

Rutinbeskrivningar och stöddokumentation förtydligar ytterligare arbetssätt som leder till att riktlinjen för informationssäkerhet uppnås.

1.2. Mål

Det huvudsakliga målet för arbetet med informationssäkerhet är att skydda kommunens verksamhet mot avbrott och minimera risken för att information används på ett felaktigt sätt. Genom åtgärder och rutiner ska informationssäkerhet upprätthållas till en lämplig nivå av de grundläggande kriterier för information som beskrivs nedan.

1.3. Syfte

Informationssäkerhet handlar om att ge kommunens information rätt skydd och omfattar

- **Riktighet** - att den skyddas mot oönskad och obehörig förändring eller förstörelse
- **Tillgänglighet** - att information är tillgänglig i förväntad utsträckning och inom önskad tid
- **Konfidentialitet** - att den inte i strid med lagkrav eller lokala överenskommelser/riktlinjer tillgängliggörs eller delges obehörig
- **Spårbarhet** - att i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt eller användare (vem, vad, när)

I praktiken innebär detta att Östhammars kommun inför styrmedel och lägger grunden för ett långsiktigt och systematiskt arbete med informationssäkerhet som ger verksamheterna stöd i hur de ska ta hand om och skydda den information som hanteras. Informationen ska vara nåbar när vi och våra intressenter behöver den. Innehållet ska vara korrekt och autentiskt, dvs. inte förvanskat. Den konfidentiella informationen ska enbart nås av eller delges den eller de personer som har behörighet att ta del av den. Vidare är spårbarheten viktig för att säkerställa att informationen inte har ändrats, eftersökts eller lämnats ut till någon obehörig.

1.4. Verksamhetsplanering

Informationssäkerhetsarbetet är även en del av kommunens totala verksamhetsplanering och riskhantering. Kommunstyrelsen fastställer vilka verksamhetsprocesser som är samhällsviktiga. Den information och de IT-system som stöder dessa processer ska ges den informationsklassning och det skydd som beskrivs i denna riktlinje.

Samtliga verksamheter ska bedriva ett systematiskt och långsiktigt arbete med att skydda informationstillgångar. Risk- och sårbarhetsanalyser och lokala handlingsplaner ska tas fram och förvaltas i enlighet med dessa riktlinjer för informationssäkerhet. Av handlingsplanerna ska framgå vilka prioriteringar och initiativ som görs avseende informationssäkerhet under innevarande år, med en inriktning för följande tre år. Planen ska ses över och vid behov uppdateras årligen med utgångspunkt i den löpande uppföljningen och analys av aktuella hot och sårbarheter. Informationssäkerheten ska löpande förbättras och arbetet effektiviseras.

Informationssäkerhet är kopplat till verksamhetsansvaret i alla led. Det betyder i praktiken att varje nämnd eller bolagsstyrelse och varje medarbetare som är ansvarig för en verksamhet också har att ansvara för informationssäkerheten i denna verksamhet.

I de fall nämnder och bolag uppdrar åt andra att hantera information ska avtalet om denna hantering omfatta sådana krav att informationen hanteras och följs upp i enlighet med dessa riktlinjer. Likaså ska utformning av skyddsåtgärder ske i enlighet med dessa riktlinjer och anpassade utifrån respektive verksamhet, uppdrag, hotbild och sårbarheter.

1.5. Kommunens information representerar stora värden

Kommuninvånarnas och verksamhetens behov av att ha tillgång till rätt information vid rätt tillfälle, kraven på integritet och sekretess samt samhällets rättsliga krav ställer höga krav på en säker hantering och användning av informationssystem. Information ses därmed som en samhällsviktig resurs som representerar stora värden för kommunen.

En effektiv och säker användning av informationen är också en förutsättning för kommunens verksamhet och för medborgarnas tilltro till kommunens förmåga att leverera en god service.

Informationstillgångar som är samhällsviktiga och verksamhetskritiska för kommunen ska klassificeras i fyra konsekvensnivåer:

- Allvarlig skada
- Betydande skada
- Måttlig skada
- Ingen eller försumbar skada

1.6. Klassning av informationstillgångar

Vid klassning av informationstillgångar ska informationens värde bedömas utifrån:

- Den funktion och betydelse för verksamheten den har och
- de konsekvenser det medför för verksamheten om informationen skulle hanteras felaktigt, försvinna eller komma i orätta händer.

Varje säkerhetsaspekt som ska användas vid analys av en informationstillgång ska värderas till någon av de fyra konsekvensnivåerna.

Säkerhetsaspekt **Konsekvensnivå**	**Riktighet (R)**	**Konfidentialitet (K)**	**Tillgänglighet (T)**	**Spårbarhet (S)**
Allvarlig – Nivå 4	Information där förlust av *riktighet* innebär allvarlig/katastrofal negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	Information där förlust av *konfidentialitet* innebär allvarlig/katastrofal negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	Information där förlust av *tillgänglighet* innebär allvarlig/katastrofal negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	Information där förlust av *spårbarhet* innebär allvarlig/katastrofal negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ
Betydande – Nivå 3	Information där förlust av *riktighet* innebär betydande negativ påverkan på egen eller	Information där förlust av *konfidentialitet* innebär betydande	Information där förlust av *tillgänglighet* innebär betydande	Information där förlust av *spårbarhet* innebär betydande

	annan organisation och dess tillgångar, eller på enskild individ	negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ
Måttlig - Nivå 2	Information där förlust av *riktighet* innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	Information där förlust av *konfidentialitet* innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	Information där förlust av *tillgänglighet* innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	Information där förlust av *spårbarhet* innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ
Ingen eller försumbar – Nivå 1	Information där det inte föreligger krav på riktighet, eller där förlust av riktighet inte medför någon eller endast försumbar negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	Information där det inte föreligger krav på konfidentialitet, eller där förlust av konfidentialitet, inte medför någon eller endast försumbar negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	Information där det inte föreligger krav på tillgänglighet, eller där förlust av tillgänglighet, inte medför någon eller endast försumbar negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild.	Information där det inte föreligger krav på spårbarhet, eller där förlust av spårbarhet, inte medför någon eller endast försumbar negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild.

1.7. Säkerhetsåtgärder

En säkerhetsåtgärd kan vara:

- **Organisatorisk**: att man fördelar ansvar, roller och mandat i organisationen så att informationen skyddas mot felaktig hantering (vem gör vad för att undvika att saker hamnar mellan stolarna).
- **Administrativ**: att man skapar styrdokument, rutiner eller liknande samt genomför utbildningar som stöd för säker informationshantering.
- **Fysisk**: att ha lås, larm, dörrar, fönster och motsvarande som skyddar information och informationssystem mot obehörig fysisk åtkomst.

- **Teknisk**: att olika IT-lösningar används för att skydda informationen, till exempel antivirus, behörighetssystem, säkerhetsloggning och säkerhetskopiering.

En säkerhetsåtgärd kan skydda mot brister i en eller flera av aspekterna (konfidentialitet, riktighet och tillgänglighet). Vid identifieringen av säkerhetsåtgärder bedöms vilken eller vilka av aspekterna som åtgärden skyddar mot brister i. Olika säkerhetsåtgärder kan också behöva kombineras för att ge tillräckligt skydd till lägsta möjliga kostnad. Exempelvis kan man kombinera utbildning (administrativ säkerhetsåtgärd) och ”phishing” via e-post med att införa skydd mot skadlig kod (teknisk säkerhetsåtgärd), för att kunna upptäcka och minska konsekvenserna av attacken (om någon ändå skulle klicka på en skadlig länk).

2. Hantering av informationssäkerhetsrisker

2.1 Riskanalyser

Den som ansvarar för verksamheten har också ett ansvar att regelbundet genomföra och dokumentera analyser av risker för verksamhetens informationstillgångar. Analysen ska avse händelser med konsekvens för såväl konfidentialitet, riktighet, tillgänglighet samt spårbarhet. Risker ska beskrivas på ett sätt som kan förstås av lekmän. Riskanalyser ska uppdateras regelbundet och i ljuset av förändringar i omvärlden och inträffade informationssäkerhetsincidenter.

Arbetssättet ska möjliggöra ett effektivt skydd för tillgångar genom att upprätthålla en aktuell bild av möjliga, oönskade händelser, inklusive åtgärdsförslag och konsekvensbedömningar.

2.2. Riskbedömning och riskhantering

Riskbedömningar ska genomföras i alla verksamheter och inkludera alla IT-system och applikationer som används. Risker som kan påverkas informationstillgångar ska bedömas och beslut fattas kring hur riskerna ska hanteras. Nödvändiga åtgärder ska vidtas för att upprätthålla rätt skyddsnivå för informationen.

Risker som inte kan undvikas, överföras eller accepteras måste minskas så att antingen sannolikheten eller konsekvensen reduceras till nivåer som gör risken tolerabel. Det är varje systemägares ansvar att ställa krav på olika aktörer, teknik och IT-leverantörer att utforma och tillämpa de skydd som behövs för att minska risken som avsett.

2.3. Kompetensutveckling

Bedömning och hantering av risker för informationstillgångar ska skyddas oavsett vilken form de har. Om det visar sig att skyddet kan kringgås är det viktigt att verksamheten har en förmåga att upptäcka det. De som arbetar med informationssäkerhet ska löpande följa med i vad som händer i omvärlden, genomföra riskanalyser och se till att de har den kunskap som behövs för att kunna agera, förebygga och hantera risker i den dagliga verksamheten.

2.4. Omvärldsbevakning

Omvärldsbevakning ska göras löpande och resultatet inkluderas i verksamhetens riskanalyser och stödjande dokument. Detta görs för att verksamheten ska vara medveten om externa hot och händelser i omvärlden som kan påverka hanteringen och skyddet av information.

2.5. Intressentanalyser

Som en obligatorisk del i informationssäkerhetsarbetet ska även intressentanalyser göras löpande. Det ska finnas dokumentation på vem som har ett intresse eller är beroende av informationen i kritiska verksamhets- och informationssystem, och vilka informationsvägar som ska användas i händelse av en incident.

2.6. Informationstillgångar

Kartläggningar ska löpande göras av de informationstillgångar som kommunens verksamheter har och hanterar. Kartläggningarna ska dokumenteras. Exempel på informationstillgångar är:

- Information

Databaser, filer, dokument, diarier, journaler, bokningssystem, föreningsregister, tidrapportering, dokumentation inom social omsorg, elevregister, personakter, utbetalningar, tomt- och bostadskö, avtal, styrsystem för vatten och avlopp, personalregister, anläggningsregister, schemaläggning, lönesystem, fakturering, redovisning, betyg, verksamhetsplaner, etcetera.

- Program

System, tillämpningar, operativsystem, abonnemang, etcetera.

- Fysiska tillgångar

Datorer, datamedia, lokala nätverk, webbservrar, etcetera.

2.7. Informationsmängd

För varje informationsmängd har kommunens medarbetare ett ansvar att fråga sig vad som skulle hända:

- Om någon obehörig kommer åt informationen.
- Om informationen är felaktig.
- Om informationen inte är tillgänglig.

2.8. Konsekvenskategorier

Exempel på konsekvenskategorier som bör användas vid konsekvenskategoriseringen:

- Ekonomisk förlust (exempelvis: minskade intäkter, ökade kostnader, skada på tillgångar)
- Negativ påverkan på, eller avbrott i, verksamheten
- Överträdelse/bristande efterlevnad av rättsliga krav
- Skadat varumärke/minskat förtroende
- Skada på annan organisation/omgivande samhället
- Personskada
- Miljöskada

2.9. Workshop som metod vid kartläggning och klassning av information

Workshopmetoden rekommenderas som lämpligt arbetssätt vid kartläggning och klassning av information. Säkerhetsskyddschef eller av denne utpekad medarbetare kan leda arbetet. Exempel på frågeställningar att behandla då information ska kartläggas och klassas.

- Vilken information hanterar vi?
- Hur klarar vi oss om vi inte kommer åt den här informationen, om vi inte kan lita på att den här informationen är korrekt, eller om någon obehörig fått tillgång till den?
- Är kategorierna och nivåerna tillräckliga för den information vi hanterar?

3. Incidenthantering

Det ska alltid finnas aktuell information, rutiner och mallar tillgängliga för medarbetare att använda vid händelse av en informationssäkerhetsincident. Dessa ska stödja en snabb, verkningsfull och korrekt hantering av hela flödet från rapportering till åtgärd samt extern rapportering.

3.1. Incidentrapportering

Alla användare, anställda och leverantörer ska göras medvetna om sin skyldighet att rapportera informationssäkerhetsincidenter. Incidenter avseende informationssäkerhet ska omedelbart rapporteras direkt både till närmaste chef och kommunens Säkerhetsskyddschef/Beredskapssamordnare via en upprättad funktionsbrevlåda.

Personuppgiftsincidenter ska även anmälas till dataskyddsombud.

Rapporteringen ska ske enligt följande:

- rutiner för incidentrapportering
- rutiner för rapportering av personuppgiftsincident

Följande innehåll ska finnas i tillhörande mallar:

- Bedömning

Bedömning av och beslut om informationssäkerhetsincidenter:
Informationssäkerhetshändelser ska bedömas och beslut ska fattas om de ska klassificeras som informationssäkerhetsincidenter. Resultaten av bedömningar och beslut ska dokumenteras detaljerat för framtida referens och verifiering.

- Incidenthantering

I de fall oväntade och oönskade händelser inträffar - som får konsekvens för tillgångar i termer av konfidentialitet, riktighet, tillgänglighet eller spårbarhet - ska kommunen utnyttja dessa händelser till att lära av det inträffade och förbättra hanteringen av sina tillgångar.

- Insamling av bevis

Kommunen ska fastställa och tillämpa rutiner för identifiering, insamling, kopiering och bevarande av information som kan tjäna som bevis. Informationen ska sparas minst till dess att allvarlighetsgraden i händelsen är helt klarlagd.

4. Hantering av lagringsmedia

4.1. Lagring

Det ska vara tydligt och klart för alla i kommunens verksamheter var medarbetare ska hantera och lagra sin digitala information. Information får endast lagras på filservrar, i verksamhetssystem och informationssystem som beslutats av kommunen. Särskilda regler gäller för e-post, mobila enheter, sociala medier, intern och extern webbplats.

4.2. Flyttbara lagringsmedia

Användning av flyttbara lagringsmedia ska i möjligaste mån undvikas. Detta för att förhindra obehörigt röjande, modifiering, avlägsnande eller destruktion av information som lagras på dessa. Exempel på flyttbara lagringsmedia är USB-minnen, externa hårddiskar, minneskort och kamera. I undantagsfall då de ändå kan behöva användas för känslig eller verksamhetskritisk information ska det finnas rutiner för vilken typ av information och klassning som får användas var, vem som får använda vilka lagringsmedier, under vilken tidsperiod och i vilket syfte.

4.3. Transport av fysiska lagringsmedia

Lagringsmedia som innehåller känslig information ska skyddas mot obehörig åtkomst, missbruk eller förvanskning under transport.

4.4. Avveckling av lagringsmedia

Lagringsmedia med känslig information ska avvecklas på ett säkert sätt när det inte längre behövs.

5. Hantering av pappersbaserad information

Varje medarbetare ansvarar för pappersbaserad information, som anteckningar, utskrifter och vad som skrivs för hand på en tavla. Den som producerar verksamhetskritisk eller känslig information är också ansvarig för att ursprunget till pappersbaserad informationen kan härledas. Om informationen är pappersbaserad och blivit registrerad - i originalhandling - i dokument- och ärendehanteringssystem (eller annat verksamhetssystem med registreringsmöjlighet) ska papperet vara märkt med registreringsnummer/diarienummer.

Om den pappersbaserade informationen är sekretessbelagd ska handläggaren tillse att den är diarieförd. Undantag finns för hemlig information. I dessa fall skall handlingen stämplas med sekretesstämpel. Se Östhammars kommuns separata riktlinjer för hemlig information.

5.1. Överföring av ”icke-digital” information

När icke-digitala informationstillgångar överförs ska den som förmedlar informationen förvissa sig om att mottagaren är den avsedda och att lämpliga skyddsåtgärder vidtagits för att säkerställa detta. Innan icke-digital information överlämnas ska mottagaren informeras om hur informationen ska hanteras och förvaras.

5.2. Förvaring
Arbetsmaterial kring pågående ärenden med personuppgifter eller sekretessbelagd eller annan känslig information bör förvaras i låsbara utrymmen, skåp eller lådor.

5.3. Avveckling
För att förstöring av pappershandlingar (allmänna handlingar) skall kunna ske måste en informations-/dokumenthanteringsplan vara beslutad av ansvarig nämnd/styrelse. Gallring ska utföras till ”sekretesstunnor” eller dokumentförstörare, placerade innanför lokalens skalskydd. Tömning av dessa ska ske regelbundet internt eller av behörig leverantör.

6. Åtkomst till informationstillgångar

6.1. Autentisering (identifiering av personer och system)
Autentiseringslösningar ska möjliggöra för endast behöriga personer och resurser att komma åt de informationstillgångar som behövs i tjänsten. Alla utställda identiteter i ett IT-system ska vara unika över tid. Åtkomsten ska vara spårbar till en fysisk person eller system. Systemägare ansvarar för att system som hanterar information - som kan leda till kritisk skada ur perspektiven riktighet, tillgänglighet och konfidentialitet - har åtkomstkontroll som baseras på autentisering med rätt tillitsnivå.

6.2. Registrering och avregistrering av användare
En formell process för registrering och avregistrering av användare ska finnas. Användare ska vara unikt identifierade.

6.3. Tilldelning av behörighet
En formell process för tilldelning av behörigheter ska finnas. Tillgång till alla informationssystem ska styras med hjälp av åtkomstkontroll.

6.4. Hantering av användares inloggningsuppgifter
Hantering av användares inloggningsuppgifter som till exempel lösenord, PIN-koder och SITHS-kort, ska ske på ett sådant sätt att uppgifterna inte röjs. Om dessa uppgifter röjs ska detta omgående anmälas och spärras. Not. I Östhammars kommun är det IT-Centrum som hanterar lösenord till datorkonton (AD) medan systemförvaltaren hanterar verksamhetssystemen.

6.5. Åtkomstkontroll till informationstillgångar
Åtkomst till information, informationssystem och tjänster ska begränsas i enlighet med systemägarens reglering. Det ska ske genom att säkerställa behörig åtkomst, förhindra obehörig åtkomst och göra användare ansvariga för att skydda sina inloggningsuppgifter.

6.6. Hantering av priviligierade åtkomsträttigheter
Åtkomst med utvidgade rättigheter, så kallade administratörsrättigheter (”admin”), ska begränsas till så få personer som möjligt. Inloggning med administratörsrättigheter ska alltid ske med ett personligt inloggningskonto. Behörigheter ska vara begränsade till vad som krävs för att utföra de arbetsuppgifter användaren har. Samma identitet bör inte användas för till

exempel drift, systemadministration och vanlig användning – om inte en säker Singel-Sign On-lösning finns införd och godkänd av IT-Centrum.

6.7. Borttagning eller justering av behörigheter och åtkomsträttigheter

Åtkomsträttigheter till information och informationssystem ska tas bort vid avslutande av anställning, avtal eller uppdrag och justeras vid förändringar. Chef som är ansvarig för anställning, avtal eller uppdrag ansvarar för att anmäla denna typ av förändring.

Det ska finnas en rutin som hanterar när medarbetare (anställda, praktikanter och inhyrda konsulter) slutar sin anställning eller uppdrag inom kommunen. Ansvarsuppgifter ska avlämnas och åtkomsträttigheter upphöra vid anställningens eller uppdragets slut. Behörighet till informationstillgångar ska baseras på användarens aktuella arbetsuppgifter och organisatoriska tillhörighet för att endast ge åtkomst till de informationstillgångar som behövs för att lösa arbetet.

Systemägare ansvarar för att det finns tillämpade rutiner för beställning, registrering, ändring och avregistrering av behörighet i respektive system. Rutinerna ska även omfatta administratörsbehörigheter. Systemägare ska granska användarnas åtkomsträttigheter periodiskt och/eller efter systemförändringar som kan påverka åtkomsträttigheterna.

I de fall leverantör eller annan organisation hanterar kommunens information ska regler för styrning av åtkomst regleras i avtal. Åtkomstkontroller ska motsvara informationens klassificering. Reglerna ska dokumenteras och vara möjliga att följa upp.

Det ska finnas en funktion som säkerställer automatisk utloggning ur IT-system alternativt aktivering av låst skärm/datorfunktion efter en viss tids inaktivitet som bedöms rimlig ur risksynpunkt för tänkt användningsområde.

6.8. Säkra in- och utloggningsrutiner

Information med hög konfidentialitet, som till exempel känsliga personuppgifter, bör skyddas med stark autentisering eller så kallad tvåfaktorsinloggning. Om åtkomst till känsliga uppgifter sker över öppet nätverk ska stark autentisering användas i kombination med att varje individ tar ansvar för säkra in- och utloggningsrutiner samt för att ingen obehörig kan ta del av informationen.

7. Användaransvar – säkert beteende

En robust och genomtänkt hantering av användares lösenord är en förutsättning för att säkra information i kommunens processer och system. Informationssystemen skall så långt som möjligt vara konfigurerade och härdade så att det inte går att kringgå säkerhetsfunktionerna.

7.1. Lösenordshantering

Alla användare har ett ansvar för att skydda sina inloggningsuppgifter. Detta för att förhindra obehörig åtkomst till information, informationssystem och tjänster.

Den som är inloggad i ett informationssystem ansvarar också för vem som tar del av informationen som aktuell inloggning ger åtkomst till.

Hantering av inloggningsuppgifter som t.ex. lösenord, PIN-koder och SITHS-kort, ska ske på ett sådant sätt att uppgifterna inte röjs. Om dessa uppgifter röjs ska detta omgående rapporteras och spärras.

Användaren ansvarar även för att:

- välja ett bra* lösenord utifrån givna anvisningar
- hålla lösenordet för sig själv
- inte återanvända lösenordet utanför tjänsten
- vara uppmärksam på missbruk av eget konto, till exempel senaste inloggning
- uppdatera sin kontaktinformation för återställande av lösenord
- hålla sig uppdaterad och använda nya säkra lösningar för inloggning där de är tillgängliga

* Ett bra lösenord är minst 9 tecken långt och svårt att gissa även för den som känner personen väl. Det innehåller både stora och små bokstäver samt specialtecken.

Systemägaren ansvarar för att:

- systemet är konfigurerat så att rätt beteende kring lösenord understöds (t.ex. att systemet inte tar emot för korta lösenord och meddelar användaren detta)
- förebygga och övervaka dålig efterlevnad, såsom delad användning av konto.

IT-Centrum ansvarar tillsammans med systemägare och systemförvaltare för att:

- ge rekommendationer till användare om vad som är lämpliga lösenord
- bevaka intrångsförsök
- dokumentera incidenter
- minska beroendet av statiska lösenord, t.ex. ”klasskonton” och generiska konton med fasta lösenord
- rapportera alla observerade eller misstänkta svagheter gällande informationssäkerheten

7.2. Källkritisk och medvetet beteende

I varje medarbetares ansvar ingår också att hålla sig uppdaterade kring information om hotbilder och hur man som individ kan skydda sig mot exempelvis skadlig kod, agera på ett källkritiskt sätt och se till att verksamhetskritisk information inte sprids till icke-behöriga personer. Att vara källkritisk innebär att du värderar den information du tar del av.

Kontrollera alltid källan och vem som skriver och förmedlar information. Dubbelkolla alltid med en oberoende källa om du är osäker på informationens äkthet. Fundera också på vem som är avsändare av informationen och vilket syfte som kan ligga bakom ett budskap. Andra ledtrådar för att förstå om en information är tillförlitlig och äkta är tidpunkten då informationen är skriven, om originalkällan är tillgänglig och om innehållet har ändrats då det

vidareförmedlats av andra, t.ex. via sociala medier. Undvik att dela med dig av information om du är osäker på om den är sann.

7.3. Allmänna handlingar

Notera och följ Östhammars kommuns riktlinjer, regler och råd för allmänna handlingar.

7.4. Distansarbete

Distansarbete avser alla former av arbete utanför kommunens lokaler och skalskydd. Information som nås, bearbetas eller lagras på distansarbetsplatser ska skyddas enligt beslutade säkerhetsnivåer på samma sätt som om arbetet utfördes i kommunens lokaler.

Privat utrustning[1] bör inte användas för hantering av kommunens information i tjänsten. Privat utrustning får inte användas vid behandling av personuppgifter, verksamhetskritisk, säkerhetsskyddad och samhällsviktig information.

All distansanslutning till IT-miljöer som är anslutna till Östhammars kommuns nätverk ska ske genom den lösning som IT-Centrum tillhandahåller (primärt VPN).

Släng aldrig verksamhetsviktig och skyddsvärd information i papperskorg eller soptunna. Allt för att säkerställa att ingen klassificerad eller hemlig information hamnar i orätta händer.

Säkerställ även att ingen obehörig person ges möjlighet att läsa information av detta slag. Ta alltid undan – och lås in – verksamhetskritisk och skyddsvärd information.

Vid arbete i hemmet sträva alltid efter att hitta en plats där du kan jobba ostört, där ingen kan lyssna på det du säger eller ta del av information via din skärm.

Vid de fall arbetsuppgifter hanterar känslig eller verksamhetskritisk information ska det ske en individuell bedömning av medarbetare och chef huruvida hemarbete är lämpligt.

7.5. Chefer

Chefer ansvarar för att informera, uppmärksamma och motivera medarbetare att ta sitt ansvar. Chefer ansvarar också för att ge det stöd som medarbetarna behöver i frågor om lämplighet att arbeta hemma.

7.6. Tillgång till nätverk och nätverkstjänster

Användare ska endast använda de nätverk och nätverkstjänster som beslutats av Östhammars kommun och som de har beviljats åtkomst till. Eget Wifi med lösenord får användas. All distansanslutning till IT-miljöer som är anslutna till Östhammars kommuns nätverk ska dock ske genom VPN (“virtuellt privat nätverk” – en tjänst som skyddar din internetanslutning och integritet på Internet).

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

7.7. Avstängning av åtkomst

Medarbetares tillgång till IT-system får stängas av vid misstanke om brott mot lag eller interna styrande dokument. Beslut om sådan avstängning ska fattas av nämnd eller bolag, eller person med delegation därifrån.

Medarbetares tillgång till IT-system får stängas av då användningen utgör en hög risk för kommunens IT-miljö och/eller informationstillgångar. Beslut om sådan avstängning ska fattas av ägaren av det nätverket, eller person med delegation därifrån. Innan beslut om avstängning fattas ska riskerna med avstängningen ha analyserats.

7.8. Installation av programvara

Okontrollerad installation av program kan leda till införande av sårbarheter och leda till obehörig åtkomst till information, förlust av riktighet, andra säkerhetsincidenter eller överträdelse av immateriella rättigheter. Regler för programinstallationer som utförs av användare ska därför upprättas och införas. Alla användare är skyldiga att efterleva dessa. Uppstår frågor om vilka program som får installeras och användas kontakta närmaste verksamhetschef eller systemförvaltning för att ta reda på vad som gäller.

Även rutiner för att styra installation av programvara på informationssystem ska finnas. Information om tekniska sårbarheter i de informationssystem som används ska löpande bevakas. Exponering för sådana sårbarheter analyseras och lämpliga åtgärder vidtas för att behandla den tillhörande risken.

7.9. Kanaler och arbetsverktyg

7.9.1. Mobil utrustning

Med mobil utrustning räknas mobiltelefoner, bärbara datorer och motsvarande. Regler och instruktioner för hantering av mobil utrustning ska finnas baserat på informationsklassning och riskbedömning. Vid användning av mobil utrustning ska stor försiktighet iakttas för att säkerställa att verksamhetsinformation inte äventyras. Det åligger var och en som använder mobila enheter i tjänst att försäkra sig om att informationen i dessa enheter skyddas för insyn och otillåten användning. Att inte låna ut mobil utrustning, att stänga av när den inte används och låsa skärmar i pauser är ett minimumkrav för säker databehandling. Kollegor kan använda en annan kommundator, men då med sin egen inloggning.

7.9.2. Mappar på servern

För mappstrukturen på kommunens filservrar finns ett regelverk beskrivet i en nätverksmapprutin för Östhammars kommun.

7.9.3 Webbläsare

Användningen av surf på Internet utöver sådant som är nödvändigt för tjänst bör ske med sunt förnuft. Tillgången till webbplatser begränsas i liten utsträckning av arbetsgivaren.

7.9.4. Sociala medier

För regler kring användningen av sociala medier, se Östhammars kommuns handbok för sociala medier.

7.9.5. E-post

Använd standard e-post med försiktighet när det gäller känslig, verksamhetskritisk och samhällsviktig information. Sekretessbelagda uppgifter får aldrig skickas via standard e-post, då den är enkel att övervaka. Om e-post ska användas för sekretessbelagd information krävs en säker e-posthantering med kryptering. Östhammars kommun tillhandahåller tjänsten Säker E-post för dem som har specifika behov. För regler kring användningen av e-post, se riktlinjer för regler och råd för allmänna handlingar och rutiner för e-postsignaturer, m.m.

7.9.6. Videokonferens

Videokonferenser kan med fördel användas för samtal om informationssäkerhet, dock bör ingen verksamhetskritisk, samhällsviktig, känslig eller sekretessbelagd delas den vägen.

8. Kommunikationssäkerhet

8.1. Hantering av nätverkssäkerhet

Nätverk ska hanteras och styras på ett sådant sätt att information i informationssystem och tjänster skyddas. Säkerhetsmekanismer, tjänstenivåer och ledningskrav vad gäller alla nätverkstjänster ska identifieras och inkluderas i avtal för nätverkstjänster, oavsett om dessa tjänster tillhandahålls internt eller som outsourcade tjänster.

8.2. Säkerhet hos nätverkstjänster

Grupper av informationstjänster, användare och informationssystem ska separeras i nätverk. Separation av nätverk kan vara så väl logisk som fysisk. Notera att nätverkstjänster omfattar anslutningar och nät med värdeskapande tjänster samt nätverkssäkerhetslösningar som t.ex. brandväggar och intrångsdetekteringssystem.

8.3. Informationsöverföring

Det ska finnas regler, rutiner och skyddsåtgärder för att skydda information vid överföring, så väl inom kommunen som till en extern enhet. Överföring av information mellan kommunen och externa parter ska vara reglerad i överenskommelser som återspeglar informationens klassning. Information som hanteras genom elektronisk meddelandehantering (t.ex. e-post, sociala medier m.m.) ska ges lämpligt skydd.

9. Roller och ansvar

Oavsett i vilken form informationen hanteras och av vem, är det alltid den som äger informationen som har ansvaret för att den behandlas på ett ändamålsenligt och säkert sätt.

- Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhetsarbete.
- Kommunchef ansvarar att tillse att kvalitets- och informationssäkerhetsarbetet bedrivs så effektivt som möjligt, genom att visa ett tydligt stöd och fördela resurser.
- Förvaltningschef ansvarar för att informations- och systemägare utses.
- Säkerhetsskyddschef och beredskapssamordnare har det strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet.

- Säkerhetsskyddschefen eller av denne utpekad medarbetare har det operativa ansvaret att leda och stödja organisationen i det löpande informationssäkerhetsarbetet.
- Varje chef ansvarar för att det finns rutiner som säkerställer att medarbetare kan efterleva kommunens regelverk för informationssäkerhet.
- Varje medarbetare har ett ansvar att uppdatera sig och följa kommunens regelverk.
- Kommunens systemägare har ansvaret för informationen. De avgör vilken information som får hanteras, hur den hanteras och av vem.
- Systemägaren ansvarar för data i system och applikationer, och dess användning. Systemen ska uppfylla informationssäkerhetskraven i förhållande till verksamhetens behov, legala krav och säkerhetskrav - och även stödja informationens klassificering.
- Dataskyddsombud, styrelser och nämnder är personuppgiftsansvariga.
- Alla som hanterar informationstillgångar har ett ansvar för att informationssäkerheten upprätthålls.

10. Leverantörsrelationer

10.1. Informationssäkerhet i leverantörsrelationer

När kommunen köper IT-tjänster av extern part eller förlägger drift av informationssystem och tjänster hos en sådan, ska minst samma regler för informationssäkerhet gälla och avtalas som när driften hanteras i egen regi.

10.2. Hantering av säkerhet inom leverantörsavtal

Alla relevanta informationssäkerhetskrav ska avtalas med varje leverantör som kan tillgå, behandla, lagra och kommunicera information eller som tillhandahåller informationssystem och tjänster till kommunen. Avtalen med leverantörer ska innehålla krav på att hantera informationssäkerhetsrisker och informationssäkerhet i linje med kommunens riktlinjer. Vid ändring av leverantörers tjänster eller avtal ska en förnyad riskbedömning genomföras.

10.3. Hantering av leverantörers tjänsteleverans

För de tjänsteleveranser som klassificeras som verksamhetskritiska ska kommunen regelbundet övervaka, granska och genomföra revision.

11. Kontinuitet för informationssäkerhet

Med kontinuitetsplanering avses den planeringsprocess som syftar till att säkerställa fortsatt verksamhet vid störningar och avbrott i informationssystem och tjänster, som beskrivs i en avbrottsplan.

Kommunens processer, rutiner och säkerhetsåtgärder ska säkerställa den nivå av kontinuitet för informationssäkerhet som anges i avbrottsplanen. Kommunen ska verifiera de fastställda och införda åtgärderna för kontinuitet av informationssäkerhet med jämna mellanrum för att säkerställa att de är giltiga och verkningsfulla under störningar.

12. Efterlevnad juridiska och avtalsmässiga krav

12.1. Identifiering av gällande lagstiftning och avtalsmässiga krav

Ansvariga för informationssystem ska löpande hålla sig uppdaterade på krav som återfinns i lagar, förordningar och avtal. Kravuppfyllnad och efterlevnad ska dokumenteras.

12.2. Immateriella rättigheter

Lämpliga rutiner ska införas för att säkerställa efterlevnad av författningsenliga och avtalsmässiga krav relaterade till immateriella rättigheter.

12.3. Skydd av dokumenterad (lagrad) information

Lagrad information ska skyddas från förlust, förstörelse, förfalskning, obehörig åtkomst och otillåten utgivning enligt informationens säkerhetsklassning, oavsett media.

12.4. Skydd av personlig integritet och personuppgifter

Enligt gällande författningar ska kommunen som personuppgiftsansvarig vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna.

12.5. Reglering av kryptografiska säkerhetsåtgärder

Kryptografiska säkerhetsåtgärder ska användas i enlighet med gällande avtal och författningar.

12.6. Särskilt skydd av personer med skyddade personuppgifter

Skyddade personuppgifter är alltid konfidentiell information och skall hanteras utifrån särskilda regler och rutiner.

13. Fysisk och miljörelaterad säkerhet

Fysisk säkerhet för kontor, rum och anläggningar ska utformas och tillämpas. Utformningen av det fysiska skyddet av informationstillgångar ska baseras på genomförda riskanalyser och vara dimensionerat utifrån tillgångarnas värde, identifierade risker och styrande regelverk. I fråga om förvaring av IT-system och nätverk är det ägaren som ansvarar för förvaringen och därmed för det fysiska skyddet.

13.1. Säkra områden

Fysiska säkerhetsavgränsningar ska definieras och användas för att skydda områden som innehåller antingen känslig eller verksamhetskritisk information, informationssystem och tjänster. Säkra områden ska skyddas genom lämpliga säkerhetsåtgärder för att säkerställa att endast behörig personal får tillträde.

13.2. Skalskydd och tillträdeskontroll

Fysiska avgränsningar ska användas för att skydda utrymmen som innehåller informationstillgångar. Utrymmen där informationstillgångar förvaras eller bearbetas ska skyddas genom lämpliga säkerhetsåtgärder för att säkerställa att endast behöriga medarbetare får tillträde till informationstillgångarna. För förvaring av informationstillgångar som kan leda

till kritisk skada ur perspektiven riktighet, tillgänglighet och konfidentialitet ska tillträdet loggas. För mer information, se Östhammars kommuns riktlinjer för hemlig information.

13.3. Utrustning och underhåll

Utrustning ska placeras och skyddas för att minska riskerna för miljörelaterade hot och faror och möjligheter för obehörig åtkomst. Utrustning ska underhållas korrekt för att säkerställa fortsatt tillgänglighet och riktighet. Utrustning i detta avseende är primärt tekniska försörjningssystem men kan även bestå av andra delar. Utrustning ska skyddas från elavbrott och andra störningar som orsakas av fel i tekniska försörjningssystem.

13.4. Kablagesäkerhet

Kablage för ström, tele- och datakommunikation bör skyddas från avlyssning, störningar och skada.

13.5. Regler för användning av kryptering

Beslut om krypteringslösning ska tas om det bedöms som en lämplig säkerhetsåtgärd baserad på informationsklassning och riskbedömning.

13.6. Hantering av kryptografiska nycklar

Rutiner för hantering av kryptografiska nycklar ska vara dokumenterad och belysa aspekter som hur nycklarna tas fram, hur de lagras och hur åtkomst ska ske.

13.7. Säkerhet för utrustning och tillgångar utanför organisationen

Säkerhet ska tillämpas på tillgångar utanför kommunens lokaler med hänsyn tagen till de särskilda risker som är förknippade med att arbeta där. All utrustning som innehåller lagringsmedia ska granskas för att säkerställa att all känsliga data och licensierade program har avlägsnats eller säkert överskrivits före kassering eller återanvändning.

13.8. Obevakad utrustning

Användare ska i samråd med chef säkerställa att obevakad utrustning har lämpligt skydd.

13.9. Skydd mot angrepp, olyckor och naturkatastrofer

Utrymmen som innehåller informationstillgångar ska ha ett fysiskt skydd mot naturkatastrofer, illvilliga angrepp eller olyckor som är anpassat till tillgångarnas värde.

14. Driftsäkerhet – drift och underhåll av informationssystem

För att undvika störningar och driftstopp i Östhammars kommuns IT-system krävs en förvaltning och drift med etablerade rutiner för driftsättning, säkerhetskopiering och loggning.

14.1. Rutiner för drift och förvaltning

Systemägare och ägare av nätverk ansvarar för att administration, drift och underhåll av IT-system sker på ett strukturerat och spårbart sätt. Systemägare av IT-system som är verksamhetskritiska ur perspektiven riktighet, tillgänglighet och konfidentialitet ska tillse att det finns en kontinuerlig övervakning under systemets drifttid/öppettid för att proaktivt upptäcka och åtgärda fel, minimera avbrott och förebygga IT-incidenter.

14.2. Test, utveckling och utbildning i IT-miljön

Produktionsdata som är skyddsvärda ur perspektivet konfidentialitet ska inte användas under test och utveckling av IT-miljön. De ska inte heller användas i utbildningsmiljö om inte utbildningsmiljön har samma skydd som produktionsmiljön. Tester av IT-miljön ska säkerställas att det inte leder till kritisk skada i produktionsmiljön.

14.3. Systemdokumentation

Systemförvaltare ska säkerställa att:

- det finns en dokumentation som ger ett tillräckligt stöd för strukturerad och säker drift och förvaltning
- användarna får kunskap om vilken typ av information som får hanteras i ett IT-system och eventuella regler kring denna hantering.
- användarna får information om att händelser i IT-systemet loggas.

14.4. Säkerhetsloggning

Systemägaren av IT-system (med hög klassning) ansvarar för att:

- händelser som kan ha betydelse för säkerheten i IT-systemet eller IT-miljön i Östhammars kommun loggas. Av denna säkerhetslogg ska tidpunkt och annan för händelsen relevant information framgå.
- det finns rutiner för hantering av systemets loggar och händelser som kan påverka säkerheten i IT-systemet. Rutinerna ska omfatta hur systemförvaltningen ska kunna upptäcka obehörig åtkomst eller annan skadlig påverkan. Rutinerna ska även omfatta vad som behövs i övrigt samt vilka åtgärder som ska vidtas vid upptäckta händelser.
- på förfrågan kunna tillgängliggöra sådana säkerhetsloggar som behövs för att kunna upptäcka och utreda hot mot och sårbarheter i skyddet
- säkerhetsloggar sparas i minst tre månader
- säkerhetsloggar sparas i minst fem år då informationen kan leda till kritisk skada

14.5. Skydd mot skadlig kod

- IT-Centrum ska säkerställa att behovet av skydd mot skadlig kod i IT-systemet är analyserat. I de fall behov av skydd mot skadlig kod finns ska ägaren av IT-systemet säkerställa att sådant skydd implementeras.

14.6. IT-infrastruktur

- Alla IT-system ska ha korrekt tidsangivelse.
- Ägaren av IT-system ska säkerställa att endast IT-system används där alla delkomponenter fortfarande supporteras av respektive leverantör. Om detta inte är möjligt ska riskerna reduceras till en acceptabel nivå.
- Leverantörers säkerhetsuppdateringar ska installeras skyndsamt i IT-system.

14.7. Styrning av ändringar i IT-system

Det ska finnas rutiner för ändringshantering och testning av IT-system.

14.8. Säkerhetskopiering och återläsning av data

Säkerhetskopiering av informationstillgångar (inklusive programvara) ska utföras regelbundet, med frekvens och omfattning anpassad till verksamhetskrav respektive legala krav, enligt fastställd instruktion. För information, som behövs för organisationens förmåga att utföra sitt uppdrag, ska säkerhetskopiering ske minst en gång per dygn.

Tester för att återskapa information från säkerhetskopior ska genomföras regelbundet och resultatet ska dokumenteras. För information som behövs för nämnden eller bolagets förmåga att utföra sitt uppdrag, ska kontroll ske minst en gång per år att uppgifterna på säkerhetskopiorna går att återskapa inom den tidsrymd som nämndens eller bolagets kontinuitetsplanering kräver. Säkerhetskopior och original ska förvaras fysiskt åtskilda i enlighet med riskbild för informationen.

14.9. Redundans

För informationssystem med hög säkerhetsnivå på tillgänglighet bör den befintliga systemarkitekturen kompletteras med redundanta enheter eller redundant arkitektur.

15. Driftrutiner och ansvar

För att upprätthålla säker och tillförlitlig tillgång till information och funktion ska administration, drift och underhåll av informationssystem ske på ett strukturerat och systematiskt sätt. Detta för att säkerställa;

- Att information, informationssystem och tjänster skyddas mot skadlig kod.
- Skydd mot förlust av data.
- Loggning av händelser och ev. säkra bevis för otillåten aktivitet.
- Korrekt och säker drift av informationssystem och tjänster.

15.1. Dokumenterade driftsrutiner

Det ska finnas systemdokumentation för varje informationssystem. Dokumentationen ska normalt bestå av system-, drift- och användardokumentation och omfatta all information som behövs för att informationssystemet ska kunna användas på ett säkert och korrekt sätt.

15.2. Ändringshantering

Förändringar i informationssystem och tjänster som påverkar informationssäkerheten ska styras, och görs också av systemförvaltarteam.

15.3. Kapacitetshantering

Användningen av resurser ska övervakas samt vid behov justeras. Prognoser av framtida kapacitetskrav ska göras för att säkerställa nödvändig systemprestanda. Likaså ska kommunens gallringsplaner finnas på plats och följas. Vid frågor, kontakta arkivarie.

15.4. Separation av utvecklings-, test- och driftmiljö

Produktionsmiljöer för verksamhetskritiska system ska vara separerade från test- och utvecklingsmiljöer. Detta för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljön.

15.5. Skydd mot skadlig kod

Upptäckande, förebyggande och återställande säkerhetsåtgärder för att skydda mot skadlig kod ska finnas, i kombination med säkerställande av en lämplig nivå av medvetenhet hos användarna. Säkerhetsskyddschef, IT-Centrum, systemägare och systemförvaltare ska - tillsammans med verksamhetens chefer - bidra till att höja medvetandenivån hos medarbetarna.

15.6. Säkerhetskopiering av information

Säkerhetskopiering av information och informationssystem ska utföras regelbundet. Kopiorna ska förvaras i olika brandceller och med implementerade skyddsåtgärder i enlighet med informationens klassificering. Tester för att återskapa information från säkerhetskopior ska genomföras regelbundet och resultatet ska dokumenteras.

15.7. Loggning

Loggning ska ske så att det i efterhand går att följa enskilda användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser. Systematiska och regelbundna stickprovskontroller – för känslig information - ska göras av loggarna. Loggarna ska sparas i enlighet med kraven på spårbarhet för det aktuella informationssystemet. Loggarna ska vara skyddade mot obehörig åtkomst och manipulation samt finnas tillgängliga utifrån verksamhetens behov.
Systemklockorna i alla relevanta informationssystem och tjänster ska synkroniseras mot en och samma referenskälla för tid.

16. Mätning och granskning

16.1. Mätning och granskning av informationssäkerhet

Uppföljningar och mätningar ska genomföras löpande för att upprätthålla rätt säkerhet.
Interna revisioner och externa oberoende granskningar ska göras löpande och när större förändringar genomförs.
Kommunledningen granskar löpande efterlevnaden av informationssäkerhetspolicyn, gällande regler och riktlinjer, standarder och eventuella andra säkerhetskrav (bl.a. fysisk säkerhet).
Informationssystem ska även granskas regelbundet avseende teknisk efterlevnad.

17. Uppföljning

Säkerhetsskyddschefen ansvarar för den löpande uppföljningen och rapporteringen till kommunledningen. Underlaget ska innefatta information om:

- Hot och förändringar i omvärlden som kan påverka informationssäkerheten
- Kompetens och efterlevnad av regler (status och behov)
- Inträffade incidenter med större påverkan på verksamheten.
- Resultat från genomförda granskningar och revisioner