Informationssäkerhet

Stödanvisning
incident- och kontinuitetshantering

Östhammars kommun

Målgrupp	Chefer och nyckelpersoner, alla kontor och verksamheter
Avsändare	Kommunledningskontoret, Digitalisering och projektledning
Dokumentansvarig	Informationssäkerhetssamordnare
Framtagen	2024-12-09
Reviderad	2026-03-05

ÖSTHAMMARS KOMMUN
– EN DEL AV ROSLAGEN

Innehåll

Innehåll

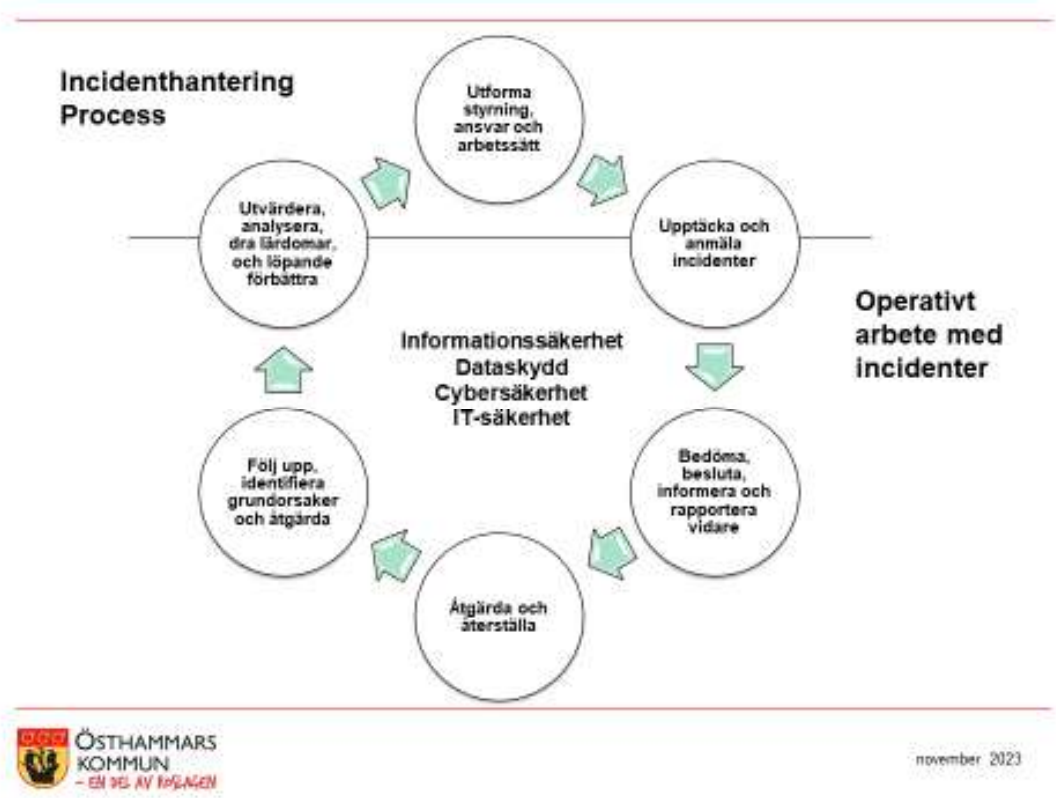
Innehållet utgår från kommunens program och vägledning för informationssäkerhet och ger en fördjupad beskrivning av kommunens process för incidenthantering och rapportering. Här ges också stödanvisningar för hur säkerhetshändelser och incidenter som påverkar/riskerar att påverka, informationssäkerheten - internt och externt. Personuppgiftsincidenter inbegrips.

Mål och syfte

Målet är en ensad process för incident- och kontinuitetshantering som svarar mot externa krav, interna behov och som bidrar till att minimera avbrott i kommunens verksamheter. Syftet är att tidigt upptäcka olika incidenter, lindra konsekvenserna av oönskade händelser och ytterst, att skydda känslig och skyddsvärd information från att komma i orätta händer, förvanskas eller förstöras. Processen understödjer ett lärande och en systematisk uppföljning.

Incidenthanteringsprocessen

Kommunens hantering av säkerhetsincidenter kopplade till informationssäkerhet och dataskydd följer processen nedan.



Utforma styrning, ansvar och arbetssätt

Nedan beskrivs det gemensamma arbetssättet vid incidenthantering/-rapportering.

Olika typer av säkerhetsincidenter

Chefer och informationssäkerhetsteamet har en viktig uppgift i att informera om vad som menas med säkerhetsincidenter, varför det är viktigt att anmäla dem och hur det ska göras. Det är varje medarbetares ansvar att anmäla inträffade incidenter, även hot och misstankar om händelser som kan leda till incidenter. När en incident inträffar är det viktigt att redan inledningsvis klara ut vilken säkerhetsincident det handlar om. Detta för att rätt person/funktion snabbt ska kunna vidta ändamålsenliga åtgärder för att lindra konsekvenserna av det inträffade. En del incidenter ska även skyndsamt rapporteras vidare till myndigheter parallellt med att berörda informeras. En **säkerhetsincident** kan vara en eller flera händelser med negativ påverkan på informationssäkerheten, det kan även vara en kombination av nedan:

En **informationssäkerhetsincident** är en enskild eller flera oönskade eller oväntade händelser som har - eller riskerar att få - negativa konsekvenser för verksamheten och dess informationssäkerhet. Även hot eller misstänkta händelser som kan vara förberedelser för någon form av cyberattack eller kriminell handling ska anmälas.
Exempel: Verksamhetskritisk och/eller samhällsviktig information - på papper, i en dator eller ett system – har kommit i fel händer, förvanskats, förstörts eller försvunnit.

En **personuppgiftsincident** är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Den kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter.
Exempel: Om en person som slutat eller bytt tjänst fortfarande har access till system som innehåller skyddsvärda personuppgifter eller om någon (med flit eller av misstag) skickar känsliga personuppgifter via en osäker kanal, som vanlig e-post.

En **IT-säkerhetsincident** berör vår IT-miljö. Den karaktäriseras oftast av att det krävs någon form av omedelbar åtgärd för att hantera en situation. *Exempel: Dator eller system beter sig konstigt, brister i virusskydd, fel i backup, misslyckad säkerhetsuppdatering, IT-haveri, etc.*

En kombination: *Exempel 1: En medarbetare glömmer en pärm på en offentlig plats. Den innehåller bl.a. en karta över vattenledningsnätet och skyddsvärda objekt. Händelsen bedöms som en informationssäkerhetsincident. Om pärmen även innehåller känsliga personuppgifter är det både en informationssäkerhets- och personuppgiftsincident.*
Exempel 2: En dator stjäls. Skärmlåset var inte på. Tyvärr tycker den som tog datorn att det är kul att sabotera – särskilt för kommunen – och hinner på kort tid både skicka massmejl och manipulera information i kritiska system. Datorn innehåller inga känsliga personuppgifter men medarbetaren har många kontakter och access till flera samhällsviktiga system. Händelsen bedöms både som en informations- och IT-säkerhetsincident.

Innan, under och efter en säkerhetsincident

Chefer har ett ansvar att hålla samman incidenthanteringen inom sin verksamhet och upprätthålla kontinuiteten på en tillräckligt god nivå. Informationssäkerhetsteamet ger tillsammans med säkerhetsskydd och beredskap stöd i processen. Dataskyddsamordnaren hjälper till vid personuppgiftsincidenter och IT-centrum vid IT-säkerhetsincidenter.

Vid en incident är det chefen för berörd verksamhet som:

- Vidtar initiala åtgärder för att minimera incidentens skadeverkning.
- Bedömer om känslig, sekretessbelagd eller annan skyddsvärd information påverkas.
- Bedömer allvarlighetsgraden, t.ex. om samhällsviktig verksamhet eller tjänst påverkas.
- Bedömer om verksamhetens kontinuitetsplan ska aktiveras.
- Hanterar incidenten på ett ändamålsenligt sätt och informerar berörda.
- Dokumenterar incidenten på ett sätt som möjliggör uppföljning och diarieföring.
- Vid behov, eskalerar incidenten till överordnad chef och kommunens krisorganisation (exempelvis allvarliga incidenter eller incidenter som drabbar fler verksamheter).
- Ser till att incidenter som kan kräva extern anmälan bedöms av kontorschef, som vid behov, i sin tur rapporterar vidare till tillsynsmyndighet.

Informationssäkerhetsteamet ger stöd genom att:

- Incidentanmälaren får återkoppling på en anmäld incident – både om det finns misstankar och hot eller om det är en faktisk incident som har inträffat.
- Den verksamhet som har drabbats - vid behov - får stöd i hanteringen av incidenten.
- Incidenten loggas. Det ska tydligt framgå vem som anmält och tagit emot incidenten, tidpunkt för anmälan, en beskrivning av incidenten, dess status och initiala åtgärder.
- I efterhand erbjuda utvärderingssamtal med berörda för att lära av det som har hänt och minimera risken för att något liknande inträffar igen.

Vid en cyber- och IT-säkerhetsincident är det IT-centrums ansvar att se till att händelser med påverkan på kommunens informationssäkerhet och dataskydd:

- Hanteras, kommuniceras, följs upp och skriftligen dokumenteras.
- Skyndsamt anmäls till informationssäkerhetsteamet och berörd/-a verksamhetschefer.
- Återföljs av utvärderingssamtal i en lärande process.

Kommunikation ger kommunikativt stöd i incident- och kriskommunikation - internt, externt och i media. Kommunikatör ingår i informationssäkerhetsteamet. En rekommendation är att involvera kommunikation tidigt i processen när något har hänt!

Kontinuitetshantering

När en incident inträffar kommer mycket kraft gå till att hantera den. Under tiden ska verksamheten upprätthållas på en tillräckligt god nivå, trots att det kanske mest kritiska och samhällsviktiga systemet inte går att nå. Det är då viktigt att ha en väl inarbetad plan B, en kontinuitetsplan, som fungerar för såväl kortvariga som långvariga störningar.

Kontinuitetsplanering görs i samband med verksamhetsplanering och en rekommendation är att öva planen innan den används i ett skarpt läge. Kontinuitetsplaner behöver alltid finnas tillgängliga för de medarbetare som förväntas använda dem. Planer med känslig och skyddsvärd information behöver förvaras inlåsta och endast behöriga personer komma åt dem.

Kontinuitetsplaner bygger på rutiner, alternativa arbetssätt och förebyggande åtgärder som behöver vidtas för att minska konsekvensen av en störning och minimera den tid som störningen påverkar verksamheten. Åtgärder kan vara fysiska, administrativa och/eller

tekniska, men de behöver svara mot de klassningskrav som ställs på Konfidentialitet, Riktighet och Spårbarhet (KRT). Kom ihåg att information även behöver skyddas och hanteras på ett lika säkert sätt vid en störning som när verksamheten löper på normalt. Säkerhetsskydd och beredskap leder kommunens kontinuitetsplanering. Informations-säkerhetsteamet stöttar i delar som rör informationssäkerhet, t.ex. systembortfall.

Upptäcka och anmäla incidenter

Upptäck incident

Ju tidigare en incident upptäcks, desto större är möjligheterna att lindra konsekvenserna av det inträffade. Det är därför lika viktigt att det tekniska varningssystemet fungerar som att vi är uppmärksamma och anmäler olika säkerhetshändelser.

Anmäl incident

Incidentanmälare är den person som anmäler en säkerhetsincident. Gör följande om en incident påverkar/riskerar att påverka informationssäkerheten och personuppgifter negativt:

- Prioritera i första hand avhjälpandet av incidenten i de fall då det är möjligt.
- Anmäl händelsen/incidenten till närmaste chef. Då närmaste chef är frånvarande, kontakta överordnad chef alt. annan tillgänglig chef.*
- Chef eller medarbetare, informera informationssäkerhetsteamet och kontorschef.
- Anmäl IT-säkerhetsincidenter direkt till IT-centrum (och till närmaste chef).
- Använd alltid anvisade kanaler*, kontaktvägar och mallar för incidentanmälan.
- Anmäl incidenten även om inte alla detaljer är kända.

*** E-tjänst för anmälan av informationssäkerhets- och personuppgiftsincidenter underlättar en samtidig rapportering till närmaste chef, kontorschef och informationssäkerhetsteamet. Använd i första hand denna e-tjänst vid incidentanmälan. Gör anmälan så snart en händelse uppdagas!**

Ta emot incidentanmälan

Incidentmottagare är den chef, medarbetare i informationssäkerhetsteamet eller på IT-centrum som tar emot en incidentanmälan. En bekräftad eller befarad incident behöver alltid följas av en informationsinsamling, återkoppling och lägesanalys – se nästa stycke.

Bedöma, besluta, informera och rapportera vidare en incident

Samla information, återkoppla och skapa en bild av läget

Vid informationsinsamling och återkoppling på en incident, ställ frågor som snabbt kan ge;

- En bra lägesbild av vad som har hänt vem, var och när.
- Fakta om känslig, sekretessbelagd eller annan skyddsvärd information röjts.
- Bild av påverkan på individer, system, processer, kritisk, samhällsviktig verksamhet
- Beskrivning av åtgärder som har vidtagits och planeras.
- Information om tidigare incidenter och ”work-around-lösningar” som kan hjälpa.

Uppmana aldrig någon att dela känslig, sekretessbelagd eller skyddsvärd information med vanlig e-post eller okrypterat videomöte. Använd kanaler och verktyg för säker kommunikation.

Bedöm allvarlighetsgraden

Gör en initial bedömning av:

- Allvarlighetsgraden, orsak och konsekvenser
- Om det rör sig om en säkerhetsincident och i sådana fall vilken typ av incident
- Om incidenten kan hanteras med ett förenklat eller särskilt förfarande.
- Om situationen behöver eskaleras till annan beslutsfattare eller expertfunktion
- Nästa steg, dvs. åtgärder, avhjälpning och skademinimering - bestäm vem som gör vad

Allvarlighetsgraden beror på vilken typ av information som har eller kan ha röjts, förstörts eller förvanskats. Bedömningen utgår från om den är verksamhetskritisk, samhällsviktig och hur informationen är klassad utifrån KRT. En högre siffra innebär en större påverkan vilket medför en högre allvarlighetsgrad vid en incident. Hur incidenterna bedöms styr sedan om de ska hanteras enligt ett förenklat eller särskilt förfarande (se förklaringen nedan).

Bedömning incident: låg allvarlighetsgrad - förenklat förfarande

En mindre incident har följande attribut och kan hanteras genom ett förenklat förfarande:

- Verksamheten påverkas endast i ringa omfattning.
- Verksamhetskritiska och samhällsviktiga informationstillgångar/system påverkas inte.
- Det föreligger ingen misstanke om att sekretess eller säkerhetskänsliga uppgifter röjts.
- Inga *känsliga* personuppgifter har röjts.
- Det föreligger ingen anmälningsplikt till extern myndighet.
- Incidenten kan relativt snabbt och enkelt avhjälpas genom ett telefonsamtal, en ändring i ett system eller en instruktion till incidentanmälaren.
- Verksamheten kan sannolikt fortsätta med ordinarie organisation och bemanning.

Vid förenklat förfarande behövs sällan någon särskild upprättad organisation för återställande och kontinuitetshantering. Ärendet behöver heller inte diarieföras. Förenklad dokumentation i form av en sammanfattning och sparad korrespondens ska dock säkerställas och sparas. Notera att en incident som är enkel att lösa tekniskt ändå kan medföra att känslig information röjs och vara anmälningspliktig. Den ska då hanteras i ett särskilt förfarande - se nästa stycke.

Bedömning incident: hög allvarlighetsgrad - särskilt förfarande

En omfattande och/eller betydande incident har ett eller flera av följande attribut och ska hanteras genom ett särskilt förfarande:

- Verksamheten påverkas i en större omfattning.
- Verksamhetskritiska och samhällsviktiga informationstillgångar/system påverkas
- Sekretessuppgifter har röjts eller det finns en misstanke om att de kan ha röjts.
- Säkerhetskänsliga uppgifter har röjts eller kan ha röjts.
- Känsliga personuppgifter har röjts eller kan ha röjts.

- Incidenten bedöms ta lång tid att avhjälpa, involvera flera verksamheter och/eller kan få en större ekonomisk påverkan.
- Det föreligger anmälningsplikt till annan myndighet.

I detta läge behöver verksamheten sannolikt använda sin kontinuitetsplan och upprätta en särskild organisation där flera olika aktörer kan samarbeta för att hantera incidenten.

Besluta

Säkerställ nödvändiga beslut så att incidenten kan hanteras och kommuniceras på ett lämpligt sätt av rätt funktion i berörd verksamhet. Försök att minimera skadeverkningarna av det som hänt och upprätthåll verksamheten på en god nivå enligt kontinuitetsplan. Beslut behövs om: Ska incidenten hanteras med ett förenklat eller särskilt förfarande? Vem behöver informeras, behöver någon varnas? Krävs anmälan till extern myndighet? Behövs resursförstärkning eller expertstöd? Bestäm vem som gör vad. Dokumentera besluten.

Vanligtvis håller ansvarig chef eller en utsedd åtgärdsansvarig[1] i incidenthanteringen. Om störningen ser ut att sprida sig, bli långdragen eller om en chef saknar befogenhet eller kompetens för att vidta åtgärder ska ärendet överföras till överordnad chef. Vid mycket ansträngande bortfall av funktionalitet och kapacitet ska krisstaben aktiveras. Vid överlämnandet ska dokumentation om vidtagna åtgärder och upprättade kontakter överföras.

Informera

Det är viktigt att - utan fördröjning - informera de som berörs eller hotas av en incident. Krisinformation ska i möjligaste mån vara målgruppsanpassad, tajmad och utgå från olika intressenters informationsbehov, och ges via redan etablerade kanaler. Det är särskilt viktigt att informera om vad de drabbade kan göra för att skydda sig i den situation som råder och var de kan vända sig för att få mer information eller stöd. Budskapen kan behöva upprepas över tid och i flera kanaler.

Det behöver framgå vad kommunen gör för att lindra konsekvenserna av det som har hänt. Ord och handling – krisinformation och åtgärder – bör gå hand i hand.
Kom ihåg att faktagranska budskap, logga informationsinsatser och informera om när incidenten är avhjälpt och verksamheten åter fungerar som vanligt.
Säkerställ att budskapen är koordinerade. Skicka endast ut varningar när de verkligen behövs!

[1] Åtgärdsansvarig är en särskilt utsedd person/roll som får i uppdrag av ansvarig chef - för den verksamhet där incidenten inträffat - att leda incidenthanteringen.

Anmäl incident till extern myndighet

En incident är anmälningspliktig om:

- Ansvarig chef har bedömt incidentens allvarlighetsgrad som hög – särskilt förfarande.
- Incidenten bedöms som betydande eller allvarlig enligt GDPR, t.ex. orsakar/kan orsaka att känsliga[2] personuppgifter röjs, förstörs, ändras eller försvinner.
- Incidenten bedöms som betydande[3] enligt NIS2 (cybersäkerhetslagen)
- Den påverkar system som stöttar tillhandahållande av hälso- och sjukvård och om den medför att hälso- och sjukvård inte har kunnat tillhandahållas i minst två timmar.
- Den påverkar system som stöttar tillhandahållande av hälso- och sjukvård och har pågått i minst sex timmar.
- Den antas påverka distribution av dricksvatten till minst 2000 personer och har pågått i minst 2 timmar.

Internt stöd i bedömningar om en incident är anmälningspliktig kan ges av informations-säkerhetssamordnare, dataskyddssamordnare och chefsjurist. Externt stöd kan ges av Myndigheten för civilt försvar (MCF), Cert-SE och dataskyddsombudet.

Rapportera säkerhetsincidenter enligt NIS2 (cybersäkerhetslagen)

Allvarliga säkerhetsincidenter enligt cybersäkerhetslagen ska rapporteras enligt:

- En första *rapport/varning* ska skickas till CERT-SE[4] via iron.msb.se *inom 24 timmar* från det att incidenten uppdagats där det framgår *om det finns misstanke om att incidenten orsakats uppsåtligen och om den kan ha gränsöverskridande effekter*.

- En *incidentanmälan* om allvarliga/betydande incidenter och cyberhot ska alltid skickas till CERT-SE inom 72 timmar från tidpunkten för kännedom. Det gäller även om incidenten *inte* är avhjälpt. Anmälan ska innehålla en inledande bedömning av dess allvarlighetsgrad, incidentens konsekvenser och förekomsten av angreppsindikatorer. Den eventuellt tidigare inskickade varningen ska uppdateras. Parallellt ska kunder som antas påverkas informeras, vid behov även om avhjälpande åtgärder.

- En slutrapport ska lämnas till CERT-SE inom en månad från incidentanmälan. Om incidenten fortfarande är pågående ska i stället en lägesrapport lämnas. Denna ska kompletteras med *slutrapport en månad efter det att incidenten har hanterats*.
  Slut- och lägesrapporter ska innehålla: en beskrivning av incidenten, hur allvarlig incidenten bedöms vara, vad som sannolikt utlöst incidenten, åtgärderna för att begränsa incidenten och incidentens möjliga gränsöverskridande effekter.

---

2 Exempel på känsliga personuppgifter enligt GDPR är etniskt ursprung, medlemskap i fackförening, hälsouppgifter och uppgifter som omfattas av sekretess enl. offentlighet- och sekretesslag (2009:400) (OSL).

3 En incident bedöms enligt NIS2/cybersäkerhetslagen som betydande om den orsakat el. kan orsaka allvarlig driftsstörning för den erbjudna tjänsten, ekonomisk skada för den berörda verksamhetsutövaren, om den påverkar el. riskerar att påverka andra fysiska eller juridiska personer genom att vålla betydande skada.

4 CERT-SE är Sveriges nationella CSIRT-enhet (Computer Security Incident Response Team) med uppgift att stötta samhället i arbetet med att hantera och förebygga IT-incidenter. Verksamheten är en del av Försvarets radioanstalt (FRA).

Här finns stöd hur rapporteringen ska ske
https://www.mcf.se/sv/amnesomraden/informationssakerhet-och-cybersakerhet/hantera-och-rapportera-it-incidenter-och-cyberangrepp/rapportera-it-incident/rapportera-en-betydande-incident-enligt-cybersakerhetslagen-nis2/

https://www.mcf.se/contentassets/295f6bac14f74c6397300152274db373/incidentanmalan-slutrapport-for-verksamhetsutovare-enligt-cybersakerhetslagen-2026.pdf

Informationsskyldighet

Om det är lämpligt ska kommunen snarast informera mottagarna av berörda tjänster om en betydande incident sannolikt påverkar tjänsterna. Vid ett betydande cyberhot ska kommunen snarast informera mottagarna av berörda tjänster som kan påverkas av hotet och om möjligt informera om skyddsåtgärder. Om det är lämpligt ska vi också informera om själva hotet. Ett cyberhot anses vara betydande om det, på grund av dess tekniska egenskaper, kan ha en allvarlig påverkan på verksamhetsutövares nätverks- och informationssystem eller orsaka användarna av tjänsterna allvarlig skada.

Rapportera personuppgiftsincident enligt GDPR

När en misstänkt personuppgiftsincident har identifierats gäller det att så snabbt som möjligt begränsa skadan, hantera omfattningen och återställa så långt det är möjligt. Detta görs genom att rapportera incidenten samt agera enligt nedanstående:

1. Det är den person som upptäcker eller misstänker en personuppgiftsincident som är ansvarig för att rapportera detta till närmaste chef.
2. Om chefen bedömer att personuppgiftsincidenten kan leda till kränkning av den enskilde ska denne kontakta dataskyddssamordnare och kontorschef.
3. Om dataskyddssamordnare inte nås ska istället dataskyddsombudet kontaktas.
4. Om kontorschefen bedömer att en extern anmälan ska göras är nästa steg att anmäla. (Chefsjurist och dataskyddsombud kan anmäla om kontorschefen inte är tillgänglig.)
5. Om incidenten bedöms utgöra en betydande eller allvarlig risk behöver de registrerade omgående informeras. Följande punkter är ett minimikrav i informationen:
   - Klar och tydlig beskrivning av personuppgiftsincidenten
   - Namn och kontaktuppgifter till dataskyddsombudet
   - Beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten
   - Beskrivning av vad kommunen har gjort eller tänker göra för att hantera incidenten som berör den registrerade - om en person behöver göra något, t.ex. byta lösenord.
6. Alla personuppgiftsincidenter ska dokumenteras och allvarliga incidenter ska även diarieföras av ansvarig chef samt tillgängliggöras för både dataskyddssamordnare och dataskyddsombudet.

Låg eller hög allvarlighetsgrad?

Det är viktigt att göra en riskbedömning av potentiella negativa konsekvenser för de drabbade registrerade personerna. Bedömningen baseras på hur stor risk det är att den enskildes integritet eller frihet kränks samt hur allvarliga dessa konsekvenser skulle kunna bli för individen.

- Låg allvarlighetsgrad: begränsad personuppgiftsincident, t.ex. enstaka namn, adresser, etc. utan koppling till mer skyddsvärda uppgifter

- Hög allvarlighetsgrad: betydande och allvarliga personuppgiftsincidenter – känsliga och skyddsvärda uppgifter, t.ex. om barn, brukare och hälsa, eller en stor mängd personuppgifter

Incidenter som bedöms utgöra en begränsad risk behöver inte anmälas till Integritetsskydds-myndigheten (IMY). Incidenter som bedömts utgöra en betydande eller allvarlig risk ska anmälas till IMY inom 72 timmar efter upptäckt samt till kommunens dataskyddsombud.

Beslutet att rapportera en incident till IMY fattas av kontorschef. Information som *inte* kan lämnas till IMY inom 72 timmar från upptäckt ska snarast kompletteras i efterhand - senast inom fyra veckor. I det fall en anmälan inte kan göras inom 72 timmar ska IMY informeras och skälen till förseningen anges. Mer information finns här:
https://www.imy.se/verksamhet/utfora-arenden/anmal-personuppgiftsincident/till-hjalp-vid-anmalan/

Undvik att lämna fler uppgifter än nödvändigt. Om någon uppgift omfattas av sekretess ska det anges vid anmälan som skickas via säker kommunikationstjänst.

Rapportera en säkerhetsskyddsincident enligt säkerhetsskyddslagen

En säkerhetsskyddsincident[5] enligt säkerhetsskyddslagen ska rapporteras skyndsamt (samma dag) till kommunens säkerhetsskyddschef samt till Säkerhetspolisen enligt särskild ordning. Detta ska göras om det finns skäl att anta att en säkerhetsskyddsklassificerad uppgift otillåtet röjts, att det har inträffat en IT-incident i ett informationssystem av betydelse för säkerhets-känslig verksamhet eller vid kännedom/misstanke om allvarlig säkerhetshotande verksamhet.

Anmäl ett brott till Polismyndigheten

Brott som t.ex. dataintrång och bedrägerier ska alltid polisanmälas. Anmälan kan göras via webben, per telefon 114 14 eller vid ett besök på en polisstation. Mer information finns här:
https://polisen.se/utsatt-for-brott/polisanmalan/polisanmalan-allt-du-behover-veta/#anmal

Informera Myndigheten för psykologiskt försvar om otillbörlig informationspåverkan

Informera Myndigheten för psykologiskt försvar (MPF) vid otillbörlig informationspåverkan från främmande makt – gäller även vid misstanke – via incident@mpf.se eller 054-52 44 90. Otillbörlig informationspåverkan är enligt MPF när främmande makt eller andra yttre hotaktörer på ett skadligt sätt försöker påverka, störa och styra det offentliga samtalet i Sverige. Några av medlen i informationspåverkan är desinformation, vilseledning och propaganda. För att något ska kunna identifieras som otillbörlig informationspåverkan behöver följande kriterier vara uppfyllda: medvetet vilseledande, avsiktlig (har avsikt att underminera det konstruktiva samtalet och den öppna debatten) och störande (stör och försvagar samhällets funktionalitet och vårt demokratiska samtal). Läs mer på https://mpf.se.

[5] Läs mer om säkerhetsskyddsincidenter och hur de ska anmälas.
https://sakerhetspolisen.se/verksamheten/sakerhetsskydd/anmalan-vid-sakerhetshotande-handelser.html

Dokumentera och diarieför

En incident ska initialt dokumenteras av incidentmottagande chef. Denna dokumentation är i ett första läge att betrakta som en ögonblicksbild som sedan behöver kompletteras i takt med att händelsen utvecklas och mer information kommer fram. Dokumentationen är viktig för att underlätta överlämningar, utredningar, uppföljningar och lärandet inför framtiden.
Vid allvarliga incidenter ska ett ärende upprättas i kommunens diariesystem. Ärendenummer ges av registraturen och ska uppges i all extern korrespondens. När incidenten är hanterad ska den gå att läsa om i sammanfattad form, dvs. fakta, genomförda åtgärder, vem som har gjort vad när, kostnader, vilka interna och externa kontakter som har tagits, informationsinsatser, etc. Bifoga incidentanmälan, relevanta loggar, rapporter och annan relevant information.
Kom ihåg att sekretessmarkera dokumentation med känsliga uppgifter.

Åtgärda och återställa

Exakt hur varje incident ska åtgärdas och återställas beror på dess omfattning, karaktär och allvarlighetsgrad. Följ verksamhetens kris- respektive kontinuitetsplan. Om dessa brister eller om en händelse utvecklas på ett sätt som ingen hade kunnat förutse, ta stöd och hjälp vid genomförandet av åtgärder, återställandet och återgången till normal verksamhet.

Följa upp, identifiera grundorsaker och åtgärda

Så snart incidenten är hanterad och verksamheten åter fungerar som vanligt igen är det dags att göra en första uppföljning av det som har hänt. Uppföljningen görs lämpligen genom att gå igenom dokumentationen från incidenthanteringen, händelseförloppet och genomförda informationsinsatser. Analysera de åtgärder som har vidtagits och tala med personer som har berörts och medverkat i arbetet. Om inte grundorsaken till händelsen har kunnat identifieras tidigare är det dags att identifiera den nu. Dokumentera och diarieför uppföljningen.
Det är viktigt att hitta orsaken och inte bara symptomen. Ofta synliggörs då ytterligare säkerhetsåtgärder som behöver införas för att undvika att incidenten upprepas. En grundorsaksanalys kan göras på olika sätt. Ett relativt enkelt sätt är att fråga sig ”varför” fem gånger eller så många gånger det krävs för att hitta en orsak. Syftet med analysen är att förstå vad som orsakat incidenten och vad som påverkat hur den utvecklats. Exempel på grundorsaker är att befintliga tekniska säkerhetsåtgärder inte gett tillräckligt skydd eller att rutiner och arbetssätt inte fungerat som det var tänkt.

Utvärdera, analysera, dra lärdomar och löpande förbättra

Allvarliga incidenter och säkerhethetsåtgärder bör även följas upp i ett senare skede (cirka 3-6 månader efter incidenten). Det är då bra att involvera de personer som har medverkat i incident- och kontinuitetshanteringen och tillsammans reflektera över vad som har gjorts bra respektive skulle kunna ha gjorts bättre. Genom att dra lärdomar av incidenter kan kommunen bli bättre rustad för framtida händelser.

Kontaktvägar

Informationssäkerhetsteamet	Funktionsbrevlåda: infosakerhet@osthammar.se (bevakas vardagar) Kontakt med informationssäkerhetsteamet via telefon görs i första hand till: • Maria Langen (informationssäkerhetssamordnare) 0173-861 08 • Håkan Åhlénius (dataskyddsamordnare) personuppgiftsincidenter 0173-854 12 • Anneli Lennström (Informationssäkerhetsteamet) 0173-862 43
Anmälan av informationssäkerhets- och personuppgiftsincidenter	Intern e-tjänst: https://sjalvservice.osthammar.se/Incidentanmalan
CERT-SE – anmäl allvarlig informationssäkerhets- och/eller IT-säkerhetsincident	Anmälan av incident görs via iron.msb.se eller per telefon 010–240 40 40. Mer info finns här: https://www.mcf.se/sv/amnesomraden/informationssakerhet-och-cybersakerhet/om-informationssakerhet/
IMY - e-tjänst och blankett för anmälan av personuppgiftsincident samt information	E-tjänsten: https://e-tjanster.imy.se/sv/anmalan Direktlänk till blanketten: blankett-anmalan-av-personuppgiftsincident.pdf (imy.se) Information: https://www.imy.se/verksamhet/utfora-arenden/anmal-personuppgiftsincident/till-hjalp-vid-anmalan/ Information: https://www.imy.se/verksamhet/utfora-arenden/anmal-personuppgiftsincident/till-hjalp-vid-anmalan/
Polisen – anmälan av brott	Polisanmäl via webbtjänst ring 114 14 eller besök en polisstation. Mer information finns här: https://polisen.se/utsatt-for-brott/polisanmalan/polisanmalan-allt-du-behover-veta/#anmal
Säkerhetspolisen – anmälan av säkerhetshotande händelser eller verksamhet	Anmälan görs till och av säkerhetsskyddschef som nås via beredskap@osthammar.se och direkt; Elin Fogelström på 0173-861 28 eller elin.fogelstrom@osthammar.se.
MPF – anmälan av otillbörlig informationspåverkan	Rapportera vid misstänkt otillbörlig informationspåverkan från främmande makt: incident@mpf.se eller ring MPF Tjänsteperson i Beredskap (TiB) på 054-52 44 90. Mer information finns på https://mpf.se.

Stöddokument, checklistor och mallar

Stödmaterial nås via Ines Incident och kontinuitet och Vägledning och stöd:

- Blanketter för intern och extern rapportering
- Mall för kontinuitetsplanering vid systembortfall
- Checklista för rapportering av personuppgiftsincident