

Gemensamma anvisningar för incidenthantering

Diarienummer: «KS-2026/00149»
Paragraf: § 83
Beslutsinstans: Kommunens ledningsgrupp
Beslutsdatum: 2026-09-03

Informationsklassning: K:0 R:1 T:1
Dokumentansvarig: Informationssäkerhetssamordnare
Giltighetstid: Tills vidare

Föregående diarienummer:
Föregående beslutsdatum:
Föregående beslutsinstans:
Föregående paragraf:

Gemensamma anvisningar för incidenthantering

Inledning

Detta dokument specificerar anvisningarna för hur incidenter ska hanteras inom Motala kommun. Detta dokument är kommunövergripande och gäller för samtliga förvaltningar och syftar till att fastställa anställdas roll i arbetet med att förebygga, upptäcka och hantera incidenter.

Vad är en incident?

Samlingsbegreppet ”incident” omfattar IT-incidenter, informationssäkerhetsincidenter och personuppgiftsincidenter, vilka beskrivs närmare nedan. En incident kan avse en av dessa typer eller en kombination av dem.

IT-incident

En IT-incident är en oplanerad händelse som påverkar driften eller tillgängligheten av IT-tjänster, system eller infrastruktur. Det behöver inte nödvändigtvis innebära ett säkerhetsproblem utan det kan vara rent tekniskt. Det kan till exempel handla om störningar i nätverket eller på en server som leder till att ett system inte är tillgängligt.

Informationssäkerhetsincident

En informationssäkerhetsincident är en incident som inträffar när skyddet av informationen inte är tillräcklig så att informationens konfidentialitet, riktighet eller tillgänglighet påverkas negativt. Det betyder att något har hänt som gör att information inte längre är helt skyddad. Det kan handla om att information riskerar eller har röjts till obehöriga (konfidentialitet), att den ändrats på ett felaktigt sätt (riktighet) eller att medarbetare inte kan komma åt den när de behöver (tillgänglighet).

Exempel på informationssäkerhetsincidenter är följande:

- ✖ Att ett brev med personuppgifter hamnar i fel brevlåda
- ✖ Felaktig ändring av uppgifter i ärende leder till felaktigt beslut
- ✖ Att en dator eller mobiltelefon tappas bort
- ✖ Ett virus i datorn ändrar innehåll i dokument eller förstör filer
- ✖ Att ett mejl med personuppgifter skickas till fel mottagare
- ✖ En anställd pratar om känsliga uppgifter så att obehöriga kan höra
- ✖ Personal råkar skriva in olika uppgifter om samma brukare i ett system
- ✖ Att ett system inte är tillgängligt när vi behöver det

- ✖ En dator slutar fungera och viktiga filer kan inte öppnas
- ✖ Strömavbrott leder till att IT-system blir otillgängliga
- ✖ En användare glömmar bort sitt lösenord och kommer inte in i ett system

Poängen är att en informationssäkerhetsincident kan vara både liten och stor. Det behöver inte alltid vara ett dataintrång – även enkla misstag som att glömma papper på fel plats kan räknas som en informationssäkerhetsincident.

Personuppgiftsincident

En personuppgiftsincident är en händelse som leder till att personuppgifter (som t.ex. namn, adress, kontaktuppgifter, personnummer, hälsouppgifter) oavsiktligt eller olagligt förstörs, förloras, ändras, röjs för obehöriga eller blir åtkomliga för obehöriga. Skillnaden mellan en personuppgiftsincident och en informationssäkerhetsincident är att en personuppgiftsincident alltid rör personuppgifter. En informationssäkerhetsincident kan däremot inträffa utan att personuppgifter berörs, så länge incidenten påverkar informationens konfidentialitet, riktighet eller tillgänglighet negativt.

Om det är en personuppgiftsincident omfattas incidenten av dataskyddsförordningen (GDPR) och särskilda åtgärder behöver vidtas enligt nedan.

Vikten av att rapportera incidenter

Att omedelbart rapportera incidenter kan vara avgörande för kommunens förmåga att skydda verksamheten, medarbetare och information om kommunens invånare. Även till synes små eller obetydliga händelser kan snabbt eskalera och få allvarliga konsekvenser om de inte hanteras i tid. Genom att anmäla incidenter direkt ger du incidentteamet möjlighet att agera snabbt, begränsa skador och identifiera grundorsaker. Hellre en rapportering för mycket än en för lite. Varje anmälan stärker vår förmåga att förebygga, lära och förbättra våra rutiner och bidrar till en informationssäkerhetsmedveten arbetskultur.

Roller och ansvar

För att hanteringen av incidenter ska fungera operativt och kunna följas upp behöver tydliga roller och deras arbetsuppgifter definieras. Dessa framgår nedan.

Förvaltningschef - ansvarar för att förvaltningen har tillräckliga rutiner och resurser för incidenthantering och att incidenter följs upp samt rapporteras på övergripande nivå. Förvaltningschefen fattar beslut om strategiska åtgärder och förvaltningsspecifika anvisningar för incidenthantering.

Verksamhets- eller enhetschef - är incidentägare för den verksamhet där incidenten inträffar och ansvarar aktivt för att incidenten hanteras ur ett verksamhetsperspektiv. Det innebär att driva intern rapportering, bedömning, åtgärder, dokumentation och uppföljning tills incidenten är avslutad. Verksamhets- eller enhetschef säkerställer även att eventuella krav på extern rapportering uppfylls. Verksamhets- eller enhetschef ansvarar för att informera verksamhet och ledning om kritiska incidenters påverkan och konsekvenser samt för att besluta om eskalering till krisledning vid behov.

Incidentanmälare – är den som upptäcker en incident, anmäler denna samt vid behov bistår Servicedesk med kompletterande information om incidenten.

Servicedesk – är incidentmottagare och en funktion i det operativa arbetet. Servicedesk tar emot, bedömer och samordnar det övergripande operativa arbetet med incidenter.

IT-enheten – tar emot och stöttar i att bedöma incidenters allvarlighetsgrad samt tillsätter lämpligt team för hantering av incidenter som rör IT. IT-enheten ansvarar för att informera IT-personal samt eventuellt incidentteam om tekniska aspekter av incidenten och samordnar budskap med verksamhets- eller enhetschef för drabbad verksamhet. Vid behov av akuta beslut har IT-enheten även mandat att eskalera incidenter till krisledning.

Incidentledare – en funktion som sammankallar och leder ett incidentteam samt ansvarar för dokumentation och upprättande av incidentrapport.

Incidentteam - genomför de åtgärder som krävs för att hantera och lösa incidenten. Gruppen består av åtgärdsansvariga, incidentledare, incidentägare och IT-enheten. Relevanta funktioner såsom informationssäkerhetssamordnare, IT-chef, dataskyddsombud och säkerhetsskyddschef kan även ingå i incidentteamet. Vid behov kan stöd från extern säkerhetspartner avropas.

Åtgärdsansvarig – arbetar med att återställa verksamheten till ett normalt tillstånd eller i alla fall så fungerande verksamhet som möjligt. Åtgärdsansvarig kan vara en roll från både IT-enheten eller kommunens verksamheter. Exempel på åtgärdsansvarig är systemförvaltare, informationssäkerhets- och dataskyddskoordinator eller tekniker.

Informationssäkerhets- och dataskyddskoordinator – har en stödjande och samordnande roll vid informationssäkerhetsincidenter i den egna förvaltningen. Koordinatören stöttar bl.a. i att rapportera incidenter och att nödvändiga åtgärder vidtas lokalt. Koordinatören deltar även i analys och uppföljning av incidenter i den egna förvaltningen samt bidrar till att förbättringsåtgärder genomförs.

Informationssäkerhetssamordnare – har en stödjande och samordnande roll vid informationssäkerhetsincidenter. Funktionen ska bistå med stöd vid bedömning av incidentens allvarlighetsgrad, ge vägledning i hanteringen och säkerställa att incidenten följer beslutade styrdokument.

Informationssäkerhetssamordnaren stödjer även rapportering och, vid behov, anmälan till berörda myndigheter samt ansvarar för att erfarenheter från incidenten tas till vara i det fortsatta förbättringsarbetet.

Dataskyddsombud - har en rådgivande och övervakande roll. Funktionen ska stödja hanteringen av personuppgiftsincidenter, ge vägledning om skyldigheten att anmäla till Integritetsskyddsmyndigheten samt säkerställa att bedömningar och åtgärder dokumenteras enligt dataskyddsförordningen.

Incidenthantering i fyra steg

För att säkerställa att incidenter får minimal påverkan på kommunens verksamheter ska nedanstående incidenthanteringsprocess följas.

Incidenthanteringsprocessen ger information om rapportering, hantering, i relevanta fall anmälan enligt lagar och förordningar samt grundorsaksanalys av incidenter.

1. Upptäcka och anmäla

1.1. När ska incidenter anmälas?

Incidenter ska anmälas när en medarbetare i kommunen vet eller misstänker att det har inträffat en incident eller identifierar risk för att det kan inträffa en incident.

1.2 Var ska incidenten anmälas?

Det finns två sätt att anmäla incidenter i kommunen, via serviceportalen eller via telefon till IT-enhetens Servicedesk. Vid mer akuta situationer, exempelvis om incidenten äventyrar verksamhetens förmåga att genomföra sitt uppdrag eller om känsliga personuppgifter har äventyrats, ska anmälan ske via telefon. Incidenter som berör Sveriges säkerhet ska omedelbart anmälas till säkerhetsskyddschefen.

1.3 Innehåll i incidentanmälan

Rapportering av en incident ska innehålla följande:

- i. Berörd verksamhet,
- ii. Kontaktperson i form av e-post och telefonnummer,
- iii. När incidenten inträffade eller upptäcktes, inklusive tidpunkt (20åå-mm-dd tt:tt),
- iv. Beskrivning av incidenten, inklusive konsekvenser (vad som har hänt),
- v. Ange system eller tjänst om dessa berörs,

- vi. Om åtgärder har vidtagits eller verksamhet avser att vidta åtgärder för att lösa, förebygga eller mildra effekterna av incidenten ska dessa anges i incidentanmälan och vem som är ansvarig för åtgärderna.

2. Bedöma och besluta

I det här steget bedöms om händelsen utgör en incident samt vilken typ av incident och allvarlighetsgrad det rör sig om. Incidentmottagaren klassificerar incidenten, sätter prioritet och säkerställer att den skickas vidare till rätt part. Incidentägaren ansvarar därefter för verksamhetsbedömningen det vill säga att bedöma hur incidenten påverkar den egna verksamheten, om reservrutiner behöver aktiveras, om extern rapportering krävs samt om incidenten behöver eskaleras till förvaltningsledning eller central krisledning. Vid behov av eskalering till krisledning se gemensamma anvisningar för Motala kommuns krisledningsorganisation.

I vissa fall kan incidenter klassas som anmälningspliktiga enligt lagar och förordningar. Frågan om incidenten omfattas av särskilda regelverk ska lyftas och dokumenteras under detta steg. Bedömningen görs med fördel i samråd med särskilda funktioner som exempelvis informationssäkerhetssamordnare eller dataskyddsombud. Det är incidentägaren som ansvarar för att genomföra anmälan till berörd tillsynsmyndighet.

3. Åtgärda och återställa

De som är åtgärdsansvariga ansvarar för att hantera incidenten och samordnar de aktiviteter som behöver göras för att normal funktion ska återställas. Beroende på typ av incident krävs olika kompetenser. Vid incidenter i IT-miljön ansvarar driftorganisationen för det tekniska återställningsarbetet, medan verksamheten bidrar med bedömningar och bekräftar att återställningen fungerar som avsett. Vid incidenter som inte berör IT-miljön, såsom förlorad information på fysiska medier, kan åtgärdsansvarig istället vara incidentägaren eller förvaltningens informationssäkerhets- och dataskyddskoordinator.

Under en incident behöver åtgärdsansvariga säkerställa att:

- i. tillräckligt många resurser med rätt kompetens arbetar med att lösa incidenten,
- ii. arbetet sker strukturerat och dokumenteras,
- iii. beslut fattas om i vilken ordning olika åtgärder ska genomföras,
- iv. det finns stöd från andra funktioner, t.ex. informationssäkerhetssamordnare, IT-säkerhetsansvarig, dataskyddsombud, IT-chef eller jurist när det behövs. Dessa behövs särskilt om incidenten kräver åtgärder som riskerar att förvärra situationen eller skapa nya incidenter,

- v. verksamhets- eller enhetschef (incidentägare) hålls uppdaterad om hur arbetet fortskrider så att nödvändiga beslut kan fattas, exempelvis om att aktivera kontinuitetshantering, begära stöd från krisstaben eller besluta om när verksamheten kan återgå till normalt arbetssätt.

3.1 Anmälan till behörig myndighet

Om incidenten omfattas av regelverk som kräver anmälan till behörig myndighet är det viktigt att någon bevakar om kraven för extern anmälan till tillsynsmyndighet eller motsvarande har uppnåtts.

3.1.1 Informationssäkerhetsincidenter

Kommunen som helhet ingår i sektorn offentlig förvaltningsentitet och omfattas av NIS2-direktivet (cybersäkerhetslagen), vilket ställer krav på att **betydande informationssäkerhetsincidenter** ska rapporteras till Myndigheten för civilt försvar. Rapporteringen ska ske enligt följande tidsordning från det att kommunen fått kännedom om incidenten: en upplysning inom 24 timmar, en incidentanmälan inom 72 timmar, därefter en lägesrapport på begäran, samt en slutrapport senast en månad efter incidentanmälan. Förutom detta tillkommer även ett krav på att informera berörda mottagare när en betydande incident eller hot kan påverka dem eller deras möjlighet att ta del av kommunens tjänster. Med betydande incident avses incidenter som orsakat eller riskerar att orsaka allvarliga driftstörningar för de tjänster kommunen erbjuder, ekonomisk skada eller riskerar att vålla andra personer betydande materiell eller immateriell skada.¹

Vid kännedom eller misstanke om en betydande incident genomförs bedömning och rapportering i samråd med kommunens informationssäkerhetssamordnare.

3.1.2 Personuppgiftsincidenter

Personuppgiftsincidenter som inte osannolikt innebär en risk för individers fri- och rättigheter ska anmälas till Integritetsskyddsmyndigheten (IMY) inom **72 timmar** från det att incidenten upptäcktes. Det är möjligt att komplettera en anmälan till IMY inom fyra veckor. Bedömning görs tillsammans med kommunens dataskyddsombud och delegationsordningen styr vilken funktion som har delegation att anmäla personuppgiftsincidenter till behörig myndighet.

När det gäller en personuppgiftsincident ska risknivån av incidenten bedömas. När risknivån är fastställd är det lättare att vidta effektiva åtgärder. En bedömning av risknivån krävs också för att avgöra om

¹ Mer information hittar du här: [MCFES 2026:8 föreskrifter om incidentrapportering och informationsskyddighet för väsentliga och viktiga verksamhetsutövare](#)

incidenten behöver anmälas till tillsynsmyndighet, och om de registrerade måste informeras.

Omständigheter att tänka på som påverkar riskbedömningen är:

- i. Om incidenten omfattar känsliga personuppgifter
- ii. Personuppgifternas art (vilka typer av uppgifter)
- iii. Om incidenten omfattar en kombination av personuppgifter
- iv. Antalet berörda personer
- v. Antalet berörda personuppgifter
- vi. Vem som eventuellt tagit del av personuppgifterna
- vii. De eventuella konsekvenserna av incidenten
- viii. Vilka typer av personer som incidenten omfattar

3.1.3 Information till registrerade vid en personuppgiftsincident

Om en personuppgiftsincident har inträffat, och incidenten bedöms innebära en hög risk för enskilda personers rättigheter och friheter, ska de registrerade informeras om incidenten utan onödigt dröjsmål. Tröskeln för att informera de registrerade är högre än den tröskel som finns för att anmäla incidenten till IMY. Bedömningen av huruvida incidenten innebär hög risk och kräver information till registrerade görs tillsammans med kommunens dataskyddsombud.

Om incidenten bedöms innebära hög risk för de registrerade är huvudregeln att information ska gå direkt till respektive registrerad. Om direkt information till respektive registrerad innebär en oproportionell ansträngning, ska allmänheten i stället informeras eller en liknande åtgärd vidtas, som på ett lika effektivt sätt informerar de registrerade.

När den registrerade informeras ska denna information finnas med:

- i. Tydlig och klar beskrivning av incidentens art
- ii. Namnet och kontaktuppgifter till dataskyddsombud eller annan kontaktpunkt
- iii. Beskrivning av de sannolika konsekvenserna av incidenten
- iv. Beskrivning av de åtgärder vi som personuppgiftsansvarig vidtagit för att mildra incidentens potentiella negativa effekter

4. Identifiera grundorsaker

När incidenten är över och normal verksamhet pågått under en period ska grundorsaken till incidenten identifieras. En grundorsaksanalys genomförs för alla incidenter som varit kritiska, exempelvis incidenter som lett till extern rapportering till tillsynsmyndighet eller som orsakat betydande avbrott i verksamheten. Tänk på att grundorsaksanalysen ska genomföras

inom en rimlig tid efter incidenten, då det finns en risk att de som har kännedom om arbetet glömmer viktiga detaljer.

4.1 Syfte

Syftet med grundorsaksanalysen är att förstå vad som orsakat incidenten och vilka faktorer som påverkat dess utveckling. Det gäller både sådant som gick bra och det som gick mindre bra. Det är viktigt att finna orsaken och inte bara symptomen och ofta synliggör grundorsaksanalyser ett antal åtgärder som behöver införas för att undvika att incidenten upprepas. Att införa åtgärder kostar tid och resurser. Prioritera åtgärder som minskar risken för att fler incidenter orsakas av samma anledning.

4.2 Hur?

En grundorsaksanalys kan göras på olika sätt. Ett sätt är att fråga "varför" så många gånger det krävs för att hitta en orsak och sedan dokumentera svaren. Det kan till exempel handla om att befintliga tekniska säkerhetsåtgärder inte gav tillräckligt skydd, att arbetssätten inte fungerade som det var tänkt eller brister i interna styrdokument och rutiner.

Som stöd används mallen för grundorsaksanalys. Analysen omfattar:

- i. summering av analysen och dess händelseförlopp,
- ii. åtgärdsförslag av kortsiktiga och/eller långsiktiga lösningar och om möjligt beräknad kostnad,
- iii. ytterligare iakttagelser och andra upptäckta risker,
- iv. uppföljningsmetod.

Det är incidentägaren som ansvarar för att tillsätta resurser för analysen samt att fatta beslut om åtgärdsförslag.

Information om incidenter

Incidenter som lett till extern rapportering till tillsynsmyndighet ska informeras av incidentägaren till den beslutsnivå som är relevant. Detta för att möjliggöra nödvändiga beslut, prioritering av resurser, samordning av åtgärder och bedömning av eventuella konsekvenser för verksamheten. All information ska spridas med beaktande av sekretess och endast till de personer som behöver den för att hantera incidenten eller fatta beslut.

Informationssäkerhetssamordnaren gör årligen en uppföljning av kommunens informationssäkerhetsincidenter som en del av ledningens genomgång. Ledningens genomgång sker enligt beskrivningen i informationssäkerhets- och dataskyddspolicyn.

Diarieföring

Samtliga handlingar som rör en incident såsom riskanalys, grundorsaksanalys och övrig dokumentation, ska diarieföras i kommunens

ärendehanteringssystem. Registreringen ska ske utan dröjsmål och följa gällande rutiner för allmänna handlingar. Vid diarieföring ska ärendemening och klassificering utformas så att känsliga uppgifter inte röjs. Eventuella sekretessbedömningar görs i samband med registrering.

Handlingar som skapas i samband med en incident diarieförs enligt följande steg:

1. Ett ärende skapas för incidenten med ett tydligt och sakligt ärendenamn, till exempel "*System XY – incident*". Namnet ska inte innehålla onödig information eller personuppgifter.
2. En initial sekretessbedömning görs i samband med att ärendet registreras. Om uppgifterna omfattas av sekretess ska detta markeras och hänvisning till bestämmelse i offentlighets- och sekretesslagen anges.
3. Ärendet registreras under ärendetypen **Incident**.
4. Alla inkommande och upprättade handlingar som rör incidenten läggs in i ärendet och registreras löpande.
5. När incidenten är färdigbehandlad avslutas ärendet och slutdatum registreras.

Då respektive nämnd är informationsägare och personuppgiftsansvariga sker diarieföring per nämnd.