

Hantering av IT- och informationssäkerhetsincident

-  Mål
-  Taxa
-  Reglemente
-  Policy
-  Plan
-  Delegationsordning
-  Riktlinje

Dokumentnamn	Dokumenttyp	Fastställd	Beslutsinstans
Hantering av IT- och informationssäkerhetsincident	Delegationsordning	2025-10-27	Kommunchef
Dokumentansvarig	Diarienummer	Reviderad	Giltig till
Informationssäkerhetssamordnare	KS 2025/331	--	--
Dokumentinformation			
Beskrivning av hantering av IT- och informationssäkerhetsincidenter.			
Dokumentet gäller för			
Alla anställda på Markaryds kommun			

Innehållsförteckning

1. Inledning	1
1.1 Omfattning	1
1.2 Regelverk.....	1
1.3 Information till Kommunstyrelsen	1
1.4 Definitioner.....	1
1.5 Allvarlighetsgrad av incident	2
2. Organisation och ansvar.....	3
2.1 Incidentanmälarer	3
2.2 Incidentägare	3
2.3 Incidentutredare	4
3. Tillvägagångsätt.....	4
3.1 Upptäcka och anmäla	4
3.2 Dokumentation av IT- och informationssäkerhetsincident	4
3.3 Bedöma.....	5
3.4 Information till berörda – kommunikation.....	5
3.5 Anmälan till andra myndigheter.....	5
3.7 Ytterligare stöd.....	6
3.8 Uppföljning av incident	6
5. Relaterade dokument	6

1. Inledning

Detta dokument syftar till att skapa en systematisk hantering av IT- och informationssäkerhetsincidenter enligt krav i cybersäkerhetslagstiftningen och Markaryds kommuns informationssäkerhetspolicy. Målet är en effektiv, systematisk och tydlig incidenthanteringsprocess.

1.1 Omfattning

Dokumentet inkluderar både mindre allvarliga incidenter och allvarliga incidenter.

1.2 Regelverk

Riktlinjen ska följa cybersäkerhetslagstiftningen som, vilken vid fastställandet av denna riktlinje, väntas träda i kraft 2026-01-15, där kommunerna ska ha ett systematiskt informationssäkerhetsarbete och en effektiv incidenthantering.

1.3 Information till Kommunstyrelsen

Kommunstyrelsen har det övergripande ansvaret för kommunens informationssäkerhetsarbete. Kommunstyrelsen får information kring IT- och informationssäkerhetsincidenter en gång per år eller vid behov. Information lämnas oavsett om incidenten är anmäld till berörda myndigheter eller ej. Ledningens engagemang är avgörande för systematiskt förebyggande arbete inom informationssäkerhet och de bör därför hållas uppdaterade kontinuerligt.

1.4 Definitioner

1.4.1 Informationssäkerhetsincident

Informationssäkerhet handlar om att rätt information ska finnas tillgänglig för rätt person vid rätt tid. En informationssäkerhetsincident innebär bland annat om informationen har spridits till en obehörig eller att informationen felaktigt har ändrats. En informationssäkerhetsincident kan även vara att informationen inte fanns tillgänglig när den behövs i verksamheten. Incidenten kan vara både fysisk och digital. Det räknas som en informationssäkerhetsincident oavsett om incidenten har skett avsiktligt eller inte.

Exempel på informationssäkerhetsincidenter:

- 1 Borttappat USB-minne med information.
- 2 Kvarglömd information på papper eller whiteboards.
- 3 Att någon pratar om något de inte ska framför andra.

1.4.2 IT-incidenter

IT-incidenter är oväntade händelser kopplat till IT-miljön som stör den normala driften av IT-tjänsten.

Exempel på IT-incidenter:

- Oanmält avbrott i verksamhetssystem
- Dataintrång
- Informationsläckage relaterad till en IT-tjänst
- Klickat på en osäker länk som kan vara ett virus

1.5 Allvarlighetsgrad av incident

En första bedömning av allvarlighetsgraden genomförs av ansvarig chef med hjälp av nedan beskrivning.

Mindre allvarliga incidenter är när få blir drabbade, vid exempelvis mindre tekniska fel i IT-stöd eller när enstaka användare inte följer användarinstruktionerna. En mindre allvarlig incident kan ha följande attribut:

- Kan snabbt avhjälpas av IT:s servicedesk genom exempelvis ett telefonsamtal, en enkel ändring i IT-stödet eller en instruktion till användaren.
- Anmälningsskyldighet till annan myndighet föreligger inte.
- Incidenten avser inte personuppgiftsincidenter enligt dataskyddsförordningen eller att personuppgiftsincidenten inte innebär en påverkan på enskildas fri- och rättigheter.
- Verksamhet och/eller invånare påverkas endast i ringa omfattning.
- Misstanke om att uppgifter som omfattas av sekretess föreligger inte.
- Låg informationssäkerhetsklass.

Allvarliga incidenter kan vara exempelvis större störningar i ett IT-system, ett längre avbrott (några timmar eller mer), dataintrång, en brand som förstör information eller infektion av skadlig kod. Med allvarliga incidenter menas incidenter som har en stor påverkan på kommunens dagliga verksamhet och även påverkar kommunens invånare negativt. Allvarliga incidenter har ett mer omfattande förfarande gällande dokumentation och organisation. En allvarlig incident har följande attribut:

- Kan inte avhjälpas snabbt av IT:s servicedesk utan kräver mer utredning.
- Anmälningsskyldighet till annan myndighet föreligger.
- Incidenter avser personuppgifter enligt dataskyddsförordningen som kan innebära en större påverkan på enskildas fri- och rättigheter.
- Verksamhet och/eller invånare påverkas inte endast i ringa omfattning.
- Misstanke om att uppgifter som omfattas av sekretess har röjts föreligger.
- Hög informationssäkerhetsklass.

2. Organisation och ansvar

2.1 Incidentanmälaren

Incidentanmälare är den medarbetare som uppmärksammar eller är inblandad i en IT- och informationssäkerhetsincident. Medarbetare har skyldighet att rapportera incidenten till ansvarig chef. Ansvarig chef anmäler incidenten på <https://etjanst.markaryd.se/incident> ifall händelsen ses som en mindre allvarlig utifrån ovan kriterier. Ta kontakt med informationssäkerhetssamordnaren eller IT-avdelningen vid behov av stöd i dokumentationen av incidenten.

Om incidenten kan leda till allvarliga konsekvenser för verksamheten eller enskilda individer ska IT-avdelningen och stabschef kontaktas direkt. Inträffar incidenten efter kontorstid ska ansvarig chef kontakta tjänsteperson i beredskap (TiB) på 0433 - 722 28 i enlighet med TiB-instruktionen.

Externa leverantörer ska genom avtal göras skyldiga att omedelbart efter upptäckt rapportera incidenter till kommunen, om inte detta redan regleras i lag. I avtalen ska det vara tydligt vem som kontaktas i kommunen vid eventuella incidenter. Kontaktpersonen ska därefter följa samma process som om incidenten skett hos kommunen, vilket innebär att rapportera in incidenten i e-tjänsten vid en misstänkt mindre allvarlig incident eller vid en misstänkt allvarlig incident kontakta IT-avdelningen, stabschef eller TiB:en.

Incidenter kan även upptäckas via omvärldsbevakning eller genom driftövervakning av Markaryds kommuns IT-miljö. Dessa incidenter ska även dokumenteras enligt mall för IT- och informationssäkerhetsincidenter. Ansvarig för dokumentationen är informationssäkerhetssamordnaren eller IT-personal. Dokumentationen används även för kvalitetsarbetet.

2.2 Incidentägare

Incidentägaren är i normalfallet den ansvarige för den verksamhet där incidenten inträffar. Om incidentägaren saknar befogenhet eller anser sig sakna kompetens att vidta åtgärder för kontinuitetshandling och återställande ska överordnad chef kontaktas. Om ärendet eskaleras kan även åtgärdsansvar flyttas till högre chef.

Incidentägaren är ytterst ansvarig för incidenten och fattar tillsammans med IT-chef, stabschef och/eller informationssäkerhetssamordnaren beslut om åtgärder för att avhjälpa incidenten. Incidentägaren ansvarar även för att kvarstående åtgärder genomförs efter att incidenten är under kontroll. Vid behov ansvarar även incidentägaren för att aktivera verksamhetens kontinuitetsplan.

Vid incidenter som har mycket stor påverkan på kommunens verksamhet kan kommunens krisledningsorganisation aktiveras. Krisledningsorganisationen aktiveras efter beslut av stabschefen.

2.3 Incidentutredare

Incidentutredaren är den som är ansvarig för informationssäkerhet på förvaltningen. Utredningen drivs av incidentutredaren med hjälp av incidentägaren, IT-avdelningen (vid digital incident), informationssäkerhetssamordnaren och eventuellt andra relevanta funktioner. Finns ingen ansvarig för informationssäkerhet på förvaltningen är informationssäkerhetssamordnaren incidentutredaren. Utredningen ska dokumenteras utifrån framtagna mallar som hittas [Incidenthantering - Insidan Markaryd](#).

En bedömning av incidenten och ett beslut om att anmäla eller inte anmäla den dokumenterade incidenten till berörda myndigheter tas i samråd mellan IT-avdelningen och Stabs- och säkerhetsavdelningen. Bedömningen ska dokumenteras och registreras i ärendet.

I Kommunstyrelsens delegeringsordning ska det framgå vem som har delegation för hantering av IT- och informationssäkerhetsincidenter samt beslut kring anmälan till relevanta myndigheter. När dokumentationen för IT- och informationssäkerhetsincidenten är komplett anses ärendet avslutat. Uppföljning av ärendet kan ske.

3. Tillvägagångsätt

3.1 Upptäcka och anmäla

- Kontorstid
 - Vid misstänkt mindre allvarlig incident – E-tjänst: <https://etjanst.markaryd.se/incident>
 - Vid misstänkt allvarlig incident – kontakta IT-chef
 - IT-chef – 0433–72019
 - Stabschef – kontakta kontakcenter via 0433–72000 som kopplar vidare
- Utanför kontorstid
 - Vid misstänkt mindre allvarlig incident – E-tjänst: <https://etjanst.markaryd.se/incident>
 - Vid misstänkt allvarlig incident - Kontakta tjänsteman i beredskap (TiB) på 0433 - 722 28

3.2 Dokumentation av IT- och informationssäkerhetsincident

Samtliga IT- och informationssäkerhetsincidenter, både mindre allvarliga incidenter och allvarliga incidenter, ska dokumenteras för att möjliggöra ett systematiskt informationssäkerhetsarbete, efterlevnad av lagstiftning samt vid kontroll av efterlevnad av tillsynsmyndighet.

När IT- och informationssäkerhetsincidenten har anmälts via e-tjänsten ”Rapportera incident” av incidentägaren ska ansvarig incidentutredare dokumentera incidenten med stöd av ”Mall för informationssäkerhetsincident” på [Incidenthantering - Insidan Markaryd](#). Den dokumenterade informationssäkerhetsincidenten ska läggas upp i ärendehanteringssystemet, oavsett om den anmäls eller inte. Vid dokumentation är det viktigt att information såsom personuppgifter,

sekretess eller känslig information kopplat till incidenten inte uppges då det kan leda till ytterligare en incident. Det krävs även en bedömning kring om dokumentet omfattas av sekretess eller inte.

Följ de instruktioner som finns i ”Vid en IT- och informationssäkerhetsincident – gör så här!”

Om personuppgifter finns med i incidenten är det viktigt att en personuppgiftsincident dokumenteras separat. Rutiner och mallar för det hittar du på [GDPR - Insidan Markaryd](#).

3.3 Bedöma

Bedömningen av incidenten är dynamisk och kan därmed ändras under incidenthanteringsgången. Första bedömning är om det rör sig om en incident eller inte och hur allvarlig incidenten är. Incidentutredaren gör bedömning utifrån Bilaga 1 – ”Bedömning av incident”. Bilagan bifogas sedan till dokumentation om incidenten.

3.4 Information till berörda – kommunikation

Mindre allvarlig incident - Ta stöd av informationssäkerhetssamordnaren och kommunikatör för eventuell information till berörda personer. Berörda personer kan vara medborgare, anställda, politiker, klienter med mera.

Allvarlig incident - Rutinen för kriskommunikation används med stöd av en kommunikatör.

3.5 Anmälan till andra myndigheter

- Rapportering till MSB – 24 h
 - Anmälan görs genom formulär på hemsidan: [Rapportera it-incident | MSB](#)
 - Under 2025 kommer rapporteringen gå över till FRA (Försvarets radioanstalt)
- Rapportering enligt Länsstyrelsen Skåne – Skyndsamt
- Polismyndigheten – Ingen tidsaspekt
 - Polisanmälan genomförs via 114 14 eller på polisens hemsida.
- Integritetsskyddsmyndigheten (IMY) – 72 h
 - Se rutin för personuppgiftsincidenter för anmälan.

Anmälan till berörd myndighet kan ha tidspress från det att man upptäckt IT- och informationssäkerhetsincidenten, specifika tidsintervall ser du ovan. Därför är det viktigt att IT- och informationssäkerhetsincidenter dokumenteras och rapporteras till delegat så snart som möjligt efter upptäckt. Anmälan skrivs ut/skannas in och registreras på samma ärende där dokumentationen av IT- och informationssäkerhetsincidenten finns.

3.7 Ytterligare stöd

Myndigheten för samhällsskydds- och beredskap (MSB) har bra information på sin hemsida om incidenter. Du kan läsa mer på [Hantera och rapportera it-incidenter och cyberangrepp | MSB](#). CERT-SE kan ge stöd vid inträffade eller pågående IT-relaterade störningar och IT-incidenter vid 010-240 40 40 eller cert@cert.se.

3.8 Uppföljning av incident

Incidentägaren ansvar för uppföljning av IT- och informationssäkerhetsincidenter. Incidentägaren kan ta stöd av IT-avdelningen och stabs- och säkerhetsavdelningen vid uppföljningen. Uppföljningen skickas därefter över till informationssäkerhetssamordnaren. Uppföljning görs med följande frågor:

- Har incidenthanteringsprocessen fungerat på ett tillfredställande sätt? Om inte vad kan utvecklas/förbättras?
 - Stödfrågor
 - Hur väl har de som anmäler incidenter förstått var de ska anmäla och vilken information de behöver beskriva? Behöver utbildningsmaterial förbättras?
 - Hur väl fungerade underlaget såsom kontinuitetsplanerna och incidentmallar?
- Har incidenthantering utförts på ett tillfredställande sätt?
 - Stödfrågor
 - Vad gjorde vi bra?
 - Vad ska vi tänka på till nästa gång?
 - Vad missades?

5. Relaterade dokument

- Informationssäkerhetspolicyn
- Mall för bedömning av en IT- och informationssäkerhetsincidenter
- Mall för dokumentation av IT- och informationssäkerhetsincidenter