KUNGÄLVS KOMMUN

Anvisning för informations-säkerhetsincidenter

Anvisning

Diarie-/dokumentnummer:	KS2023/1939
Beslut:	2023-11-30, Förvaltningsledningen
Ersätter tidigare beslut	2022-06-28 Förvaltningsledningen (KS2022/1221-4)
Giltighetstid:	2026-12-31
Dokumentansvarig:	HR
Senast uppdaterad av:	Informationssäkerhetssamordnare

KUNGÄLVS KOMMUN

Innehållsförteckning

KUNGÄLVS KOMMUN

1. Inledning

Kungälvs kommun ska ha en samlad funktion och organisation för incidenthantering i informationssystem. En incident är en oönskad händelse med negativa konsekvenser och mer specifikt är en informationssäkerhetsincident en incident som inträffar när skyddet av informationen inte är tillräckligt så att informationens konfidentialitet, riktighet eller tillgänglighet påverkas negativt.

En särskild lathund har upprättats för att stötta incidentmottagare och åtgärdsansvarig i sitt arbete med incidenthantering. Den finns med som bilaga (Bilaga 1) till detta dokument.

2. Relation till andra styrdokument

Informationssäkerhetspolicy
Riktlinjer för informationssäkerhet
Tillämpningsanvisning för hantering av säkerhetsklassificerade uppgifter
Lednings- och kommunikationsplan vid kriser

3. Syfte

Tillämpningsanvisningen ska tillse att kommunen har en effektiv, rättssäker och robust hantering av informationssäkerhetsincidenter.

4. Mål och viljeinriktning

Kommunens incidenthantering ska tillse att eventuella informationssäkerhetsincidenter minimerar skadeverkningar på informationens konfidentialitet, riktighet och tillgänglighet.

5. Organisation

Nedan redovisas ansvar och roller vid informationssäkerhetsincidenter.

- **Incidentanmälare.** Medarbetare eller extern som uppmärksammar en pågående incident. Medarbetaren har en skyldighet att rapportera incident till incidentmottagare omedelbart vid upptäckt.

  Externa leverantörer ska genom avtal göras skyldiga att rapportera incidenter till kommunens incidentmottagare omedelbart vid upptäckt om detta inte redan regleras i lag. Anmälan görs via incidentanmälningsformulär på kommunens e-tjänsteplattform, om detta inte är möjligt så görs anmälan via telefon. Incidentanmälare ska fylla i särskilt formulär för dokumentation av händelse.

- **Incidentmottagare.** Systemförvaltargruppen är gemensamt incidentmottagarfunktion under kontorstid, övrig tid ansvarar tjänsteman i beredskap. Incidentmottagaren genomför en första bedömning om anmälan avser en incident eller supportärende. Vid bedömning att anmälan gäller supportärende vidarebefordras ärendet till ordinarie supportorganisation. Incidentmottagare samordnar initiala åtgärder för att skademinimera incidentens skadeverkning i väntan på att åtgärdsansvarig (samt kommunjurist vid personuppgiftsincidenter) kan kontaktas och sättas in i ärendet. Incidentmottagare hanterar mindre incidenter. Incidentmottagare påbörjar dokumentation och säkerställer att underlag i form av loggar, anmälningsformulär samt övrig korrespondens dokumenteras.

- **Åtgärdsansvarig.** Åtgärdsansvarig för incidenter är chef för berörd verksamhet. Vid incidenter som påverkar mer än en enskild verksamhet inom samma sektor överförs åtgärdsansvaret till sektorchef. För incidenter i informationssystem som är kommunövergripande ansvarar respektive stabsenhetschef för åtgärdsansvaret. Om åtgärdsansvarig saknar befogenhet eller anser sig sakna kompetens att vidta åtgärder för

kontinuitetshantering och återställande ska överordnad chef kontaktas. Ärendet eskaleras och åtgärdsansvar flyttas till högre chef.

Vid mycket ansträngande bortfall av funktionalitet och kapacitet ska kommunens krisorganisation aktiveras genom tjänsteman i beredskap.

Åtgärdsansvarig ansvarar för att berörda funktioner utanför den egna verksamheten, inklusive förvaltningsledning och kommunstyrelse, hålls underrättad med relevant information om incidentarbetet. Informationssäkerhetssamordnare ska kontinuerligt hållas underrättad om incidentarbetet.

Åtgärdsansvarig ansvarar för att begränsa incidentens påverkan på verksamheten, att skyndsamt återställa normal funktionalitet och kapacitet, upprätta åtgärdsorganisation samt för kontakt med myndigheter efter att incidentmottagaren överlämnat incidenten till åtgärdsansvarig.

Efter att incidenten har åtgärdats ska åtgärdsansvarig upprätta en rapport om incidentens grundorsaker samt ge förslag på åtgärder som ska tillse att incidenten inte upprepas.

6. Hantering av incidenter

Informationssäkerhetsincidenter delas in i två kategorier, liten och stor incident. Liten incident har ett förenklat förfarande gällande dokumentation och organisation. Den har följande attribut:

- Kan snabbt avhjälpas av enbart incidentmottagare genom exempelvis ett telefonsamtal, enkel ändring i informationssystem eller instruktion till anmälaren
- Anmälningsplikt till annan myndighet föreligger inte
- Incidenten avser inte personuppgiftsincidenter enligt dataskyddsförordningen.
- Verksamheten påverkas endast i ringa omfattning
- Misstanke om att sekretess röjts föreligger inte

Vid förenklat förfarande behöver inte åtgärdsansvarig kontaktas och åtgärdsansvarig ska inte heller upprätta organisation för återställande och kontinuitetshantering. Ärende behöver inte upprättas i diariet. Förenklad dokumentation i form av korrespondens ska dock sparas under 1 års tid i E-tjänsten.

Stor incident har ett mer omfattande förfarande gällande dokumentation och organisation. Den har följande attribut:

- Kan inte snabbt avhjälpas av enbart incidentmottagare utan kräver mer utredning.
- Anmälningsplikt till annan myndighet föreligger.
- Incidenten avser personuppgiftsincidenter enligt dataskyddsförordningen.
- Verksamheten påverkas inte endast i ringa omfattning.
- Misstanke om att sekretess röjts föreligger.

En åtgärdsansvarig behöver kontaktas och hen kan behöva upprätta organisation för återställande och kontinuitetshantering. Ärende behöver upprättas i diariet och dokumentation i form av korrespondens och kontakter som gjorts behöver dokumenteras.

7. Dokumentation

En incident ska dokumenteras av incidentmottagare så snart som möjligt efter att den uppmärksammats i syfte att underlätta för utredning, rättsliga krav samt överlämning mellan incidentmottagare och åtgärdsansvarig. Historisk dokumentation kan även hjälpa

organisationen att uppmärksamma trender i verksamheten eller specifika system som behöver uppmärksammas särskilt. Ärende upprättas så snart det är möjligt i kommunens diariesystem. Om incident inträffar utanför kontorstid ska dokumentation föras in i ärende så snart detta är möjligt.

I dokumentationen ska bland annat följande framgå:

- Upprättade interna och externa kontakter tagna via telefon
- Genomförda åtgärder
- Relevant intern och extern skriftlig kommunikation
- Kommunikation med tillsynsmyndigheter
- Rapporter
- Relevanta loggar
- Anmälningar

Anmälan till driftleverantör görs av incidentmottagare genom anmälan på Soltaks kundservicesida eller till aktuell driftsleverantör för systemet.

8. Anmälan till extern myndighet

Om incidenten har påverkan på system, processer eller verksamheter som kräver incidentanmälan till externa myndigheter ansvarar incidentmottagaren för detta.

- Bortfall av samhällsviktig tjänst enligt NIS-direktivet rapporteras till Myndigheten för samhällsskydd och beredskap/CERT-SE inom 6 timmar från det att incidenten uppdagats. En andra rapportering ska ske inom 24 timmar. I korthet gäller detta system som används inom verksamhet hälso- och sjukvård och dricksvatten produktion.
- En personuppgiftsincident ska rapporteras till Integritetsskyddsmyndigheten av kommunjurist inom 72 timmar från incidentens uppdagande. Incidentmottagare vidarebefordrar anmälan till kommunens jurister.
- En säkerhetsskyddsincident gäller informationstillgångar som omfattas av säkerhetsskyddslagen och ska rapporteras till Säkerhetspolisen skyndsamt. Vid misstanke om att system som omfattas av säkerhetsskyddslagen har påverkats med avseende på konfidentialitet, tillgänglighet, riktighet eller spårbarhet kontaktas säkerhetsskyddschef.

Vid misstanke om röjande av sekretessuppgifter ska polisanmälan upprättas och inges till polismyndigheten. För detta ansvarar åtgärdsansvarig.

9. Levandegöra

Anmälningsvägar för incidentanmälare ska publiceras på intranätet under en egen kategori. Anvisning ska även publiceras på kommunens hemsida. Chefer bör även med viss kontinuitet påminna sina verksamheter via exempelvis APT om hur dom ska gå till väga för att anmäla en informationssäkerhetsincident.

10. Uppföljning

Styrdokumentet följs upp och vid behov förbättras i samband med att styrdokumentets giltighetstid löper ut.

KUNGÄLVS
KOMMUN

KUNGÄLVS KOMMUN

Bilaga 1

Lathund för incidentrapportering

Innehåll

KUNGÄLVS KOMMUN

Roller

Incidentanmälaren

Den anställda, leverantör eller konsult som anmäler incidenten till incidentmottagare. Anställda, leverantörer eller konsulter har en skyldighet att så snart som möjligt anmäla en möjlig incident till incidentmottagare.

Incidentmottagare

Systemförvaltargruppen är incidentmottagare under kontorstid, övrig tid ansvarar tjänsteman i beredskap. Genomför en första bedömning om anmälan avser en incident eller supportärende. Vid bedömning att anmälan gäller supportärende vidarebefordras ärendet till ordinarie supportorganisation. Incidentmottagare samordnar initiala åtgärder för att skademinimera incidentens skadeverkning. Vid personuppgiftsincidenter enligt dataskyddsförordningen bedömer kommunjurist om det är fråga om en anmälningspliktig incident.

Atgärdsansvarig

Åtgärdsansvarig för incidenter är chef för berörd verksamhet. Vid incidenter som påverkar mer än en enskild verksamhet inom samma sektor överförs åtgärdsansvaret till sektorchef. För incidenter i informationssystem som är kommunövergripande ansvarar respektive stabsenhetschef för åtgärdsansvaret. Om åtgärdsansvarig saknar befogenhet eller anser sig sakna kompetens att vidta åtgärder för kontinuitetshantering och återställande ska överordnad chef kontaktas. Ärendet eskaleras och åtgärdsansvar flyttas till högre chef. Vid mycket ansträngande bortfall av funktionalitet och kapacitet ska kommunens krisorganisation aktiveras genom tjänsteman i beredskap.

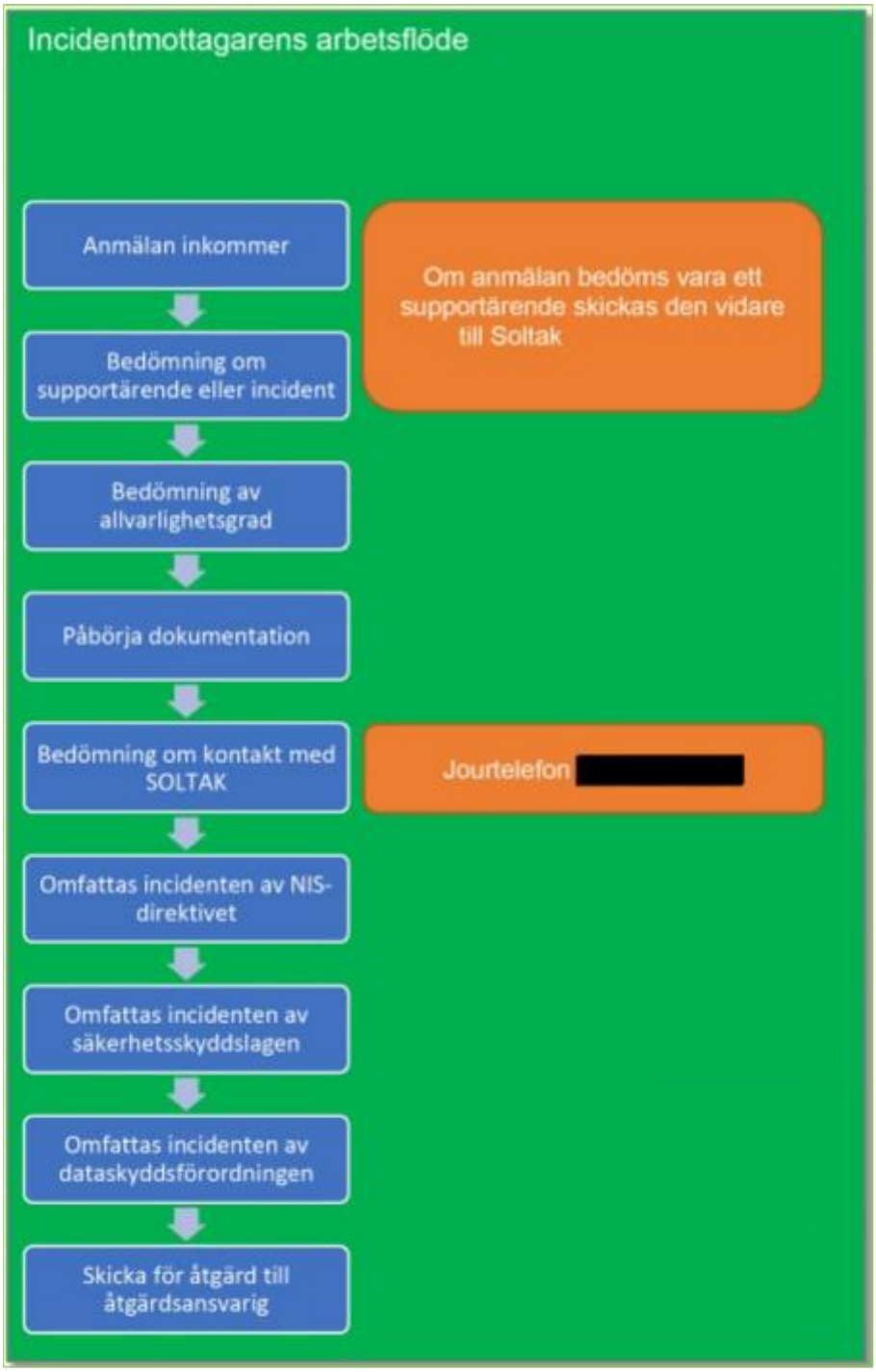
Åtgärdsansvarig ansvarar för att begränsa incidentens påverkan på verksamheten, att skyndsamt återställa normal funktionalitet och kapacitet, upprätta åtgärdsorganisation samt för kontakt med myndigheter efter att incidentmottagaren överlämnat incidenten till åtgärdsansvarig.

Arbetsflöden

Arbetsflödet efter att incidentanmälaren har lämnat in sin anmälan kan delas upp i två delar. En för Incidentmottagaren och en för Åtgärdsansvarig. Här följer beskrivning av de olika flödena och deras delar.

KUNGÄLVS KOMMUN

Incidentmottagaren



KUNGÄLVS KOMMUN

Anmälan inkommer

Efter att incidentanmälaren har skickat in sin anmälan så kan incidentmottagaren läsa den i stödsystemet och påbörja arbetet.

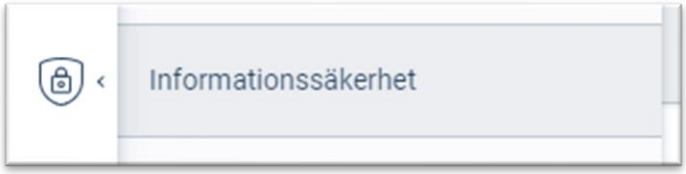
Bedömning om supportärende eller incident

Incidentmottagaren gör en första bedömning för att avgöra om det handlar om en faktisk informationssäkerhets- eller personuppgiftsincident eller ett supportärende. Om det är ett supportärende skall mottagaren skicka ärendet vidare genom vanliga supportvägar till Soltak.

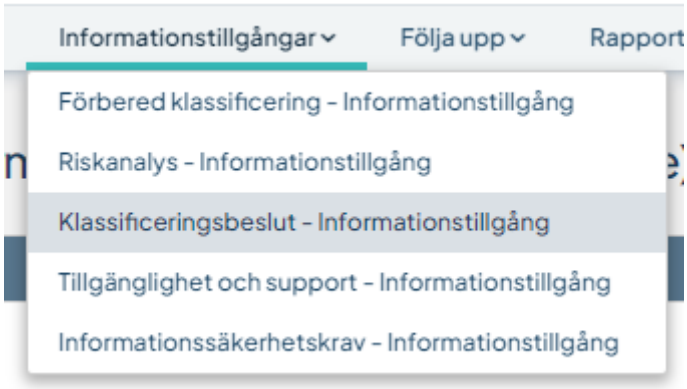
Bedömning av allvarlighetsgrad

Kommunens informationstillgångar är klassade i enlighet med en konsekvensbedömning som graderar hur viktigt den enskilda informationstillgången är för kommunens verksamhet och för samhället i stort. Informationstillgångarna är graderade efter krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet. En högre siffra innebär större påverkan på organisationen eller samhället och därmed en högre allvarlighetsgrad.

- Logga in på https://kungalv.app.stratsys.com/
- Klicka på skölden i menyn på vänster sida
- Klicka på ”Informationssäkerhet”



- Klicka på ”Informationstillgångar” och sedan ”Klassificeringsbeslut – Informationstillgång”



- Sök fram aktuell informationstillgång, de är graderade mellan 0 - 3 i kategorierna konfidentialitet, riktighet, tillgänglighet och spårbarhet. Ett högt sammanlagt värde innebär att systemet är viktigt för verksamheten eller samhället medan ett lågt värde innebär att systemet har en lägre vikt för verksamheten eller samhället.

Informationssäkerhetsincidenter indelas i två kategorier, liten och stor incident. Liten incident har ett förenklat förfarande gällande dokumentation och organisation. Den har följande attribut:

- Kan snabbt avhjälpas av enbart incidentmottagare genom exempelvis ett telefonsamtal, enkel ändring i informationssystem eller instruktion till anmälaren
- Anmälningsplikt till annan myndighet föreligger inte

- Incidenten avser inte personuppgiftsincidenter enligt dataskyddsförordningen.
- Verksamheten påverkas endast i ringa omfattning
- Misstanke om att sekretess röjts föreligger inte

Vid förenklat förfarande behöver inte åtgärdsansvarig kontaktas och åtgärdsansvarig ska inte heller upprätta organisation för återställande och kontinuitetshantering. Ärende behöver inte upprättas i diariet. Förenklad dokumentation i form av korrespondens ska dock sparas under 1 års tid. Notera att en incident som är enkel att lösa tekniskt ändå kan vara anmälningspliktig till extern myndighet. Om så är fallet ska incidenten inte räknas som enkel.

Stor incident har ett mer omfattande förfarande gällande dokumentation och organisation. Den har följande attribut:

- Kan inte snabbt avhjälpas av enbart incidentmottagare utan kräver mer utredning.
- Anmälningsplikt till annan myndighet föreligger.
- Incidenten avser personuppgiftsincidenter enligt dataskyddsförordningen.
- Verksamheten påverkas inte endast i ringa omfattning.
- Misstanke om att sekretess röjts föreligger.

En åtgärdsansvarig behöver kontaktas och hen kan behöva upprätta organisation för återställande och kontinuitetshantering. Ärende behöver upprättas i diariet och dokumentation i form av korrespondens och kontakter som gjorts behöver dokumenteras.

Påbörja dokumentation

Dokumentation av pågående incident är av stor vikt för samordning och senare utredning. I samband med att incident rapporteras in och inte anses vara en mindre incident ska begäran om ett ärende skickas till registrator@kungalv.se av incidentmottagare. Ärendenamn "Incident - [verksamhetsområde eller system]. Medhanläggare bör initialt vara åtgärdsansvarig. Ärendenumret ska anmälas i kontakt med andra myndigheter, exempelvis vid NIS-anmälan.

Incidentmottagare bör så snart det är möjligt börja dokumentera händelsen i ärendet. Om incident sker utanför ordinarie arbetstid dokumenteras ärende på annat sätt och tillförs ärende vid en senare tidpunkt. Vid överlämning av ansvar för incident till åtgärdsansvarig överförs även ärendet till denne.

Notera att uppgifter kopplade till en incident kan omfattas av sekretess med tanke på tekniska eller administrativa sårbarheter, verksamhetens kapacitet eller funktionalitet under pressade förhållanden eller liknande.

Anmälan till driftleverantör görs av incidentmottagare genom anmälan på Soltaks kundservicesida (https://kundservice.soltakab.se/) i de fall systemen finns där annars sker anmälan till annan driftsleverantör för systemet. Se listan för alla verksamhetssystem för kontaktuppgifter.

Bedömning om kontakt med Soltak

I vissa fall är det bråttom med att få kontakt med Soltak eller annan leverantör, till exempel när man misstänker att det är ett pågående intrång eller utpressningstrojan (Ransomware), ska deras jour kontaktas under kvällar och helger och den vanliga IT-supporten under dagtid. Detta för att noteras om den pågående incidenten så snabbt som möjligt.

I övriga fall kontaktas leverantören via den väg man bedömer är snabbast.

KUNGÄLVS KOMMUN

Rapportering av incidenter enligt NIS-direktivet

Anmälan av incident enligt NIS-direktivet ska ske senast sex timmar efter att incidenten uppdagats. Rapportering i steg 1 görs av incidentmottagare i MSB:s verktyg (iron.msb.se). Vid behov av stöd kontaktas CERT-SE på telefonnummer **010-240 40 40**. Incidenten är anmälningspliktig om:

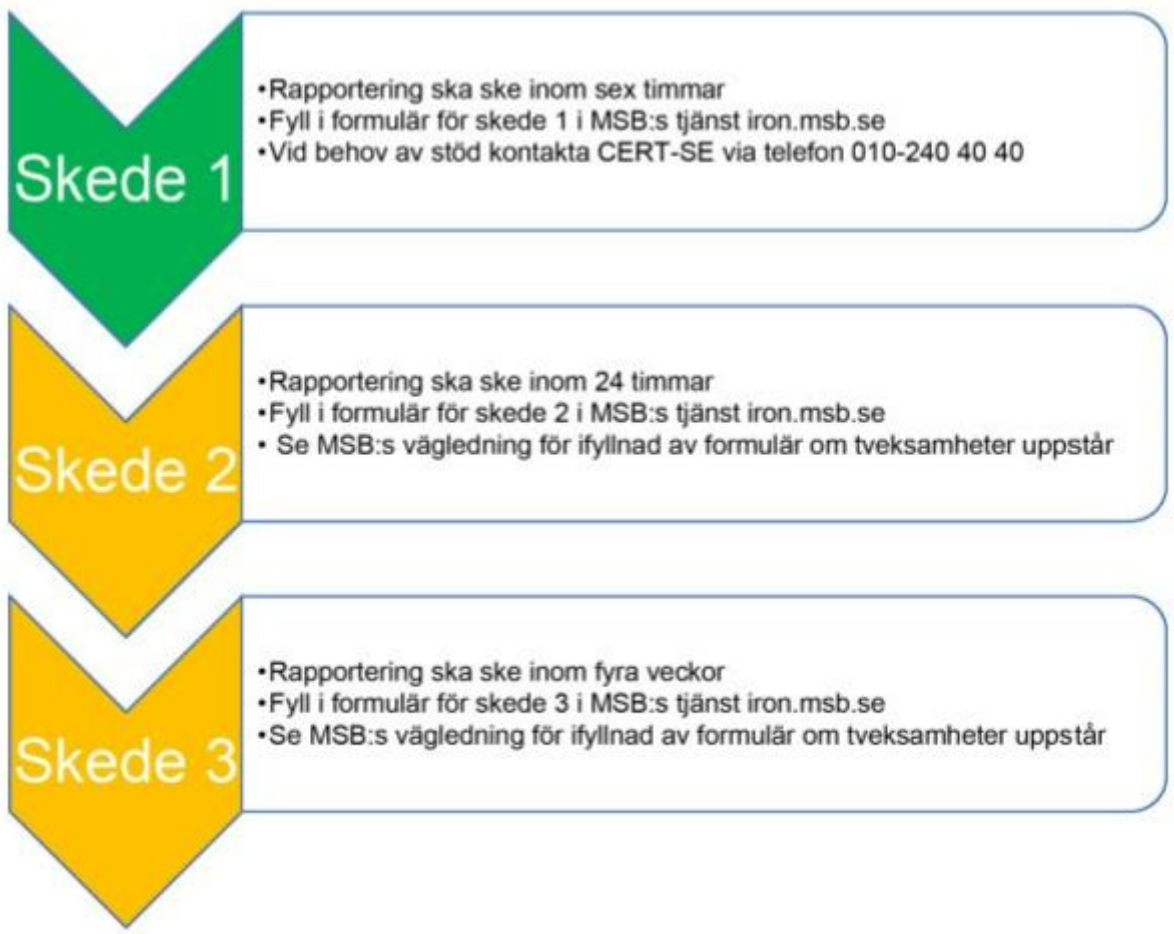
Incidenten påverkar system som stöttar tillhandahållande av hälso- och sjukvård och om incidenten medför att hälso- och sjukvård inte har kunnat tillhandahållas i minst två timmar

- Incidenten påverkar system som stöttar tillhandahållande av hälso- och sjukvård och har pågått i minst sex timmar
- Incidenten resulterar eller kan komma att resultera i en anmälan om allvarlig vårdskada till Inspektionen för vård och omsorg (IVO) enligt patientsäkerhetslagen
- Incidenten antas påverka distribution av dricksvatten till minst 2000 personer och har pågått i minst 2 timmar

Informationssystem som anses stötta hälso- och sjukvården eller distribution och leverans av dricksvatten i kommunen definieras brett. Om ett informationssystem inte uppför sig som förväntat samt resulterar i att anmälningsplikt enligt ovanstående fyra punkter aktualiseras ska anmälan göras. Notera att en anmälan gällande distribution eller leverans av dricksvatten även kan aktualisera en anmälan om säkerhetshotande händelse och verksamhet till Säkerhetspolisen.

Nedanstående system (14 st) är särskilt identifierade som viktiga för tillhandahållande av hälso- och sjukvård eller distribution och leverans av dricksvatten:

- TES
- Samsa
- Trygghetslarmet - ordinärt boende
- Phoniro
- MCSS
- NPÖ - nationell patientöversikt
- CactusEye
- Treserva
- HSA-katalogen
- Trygghetslarmet - särskilt boende
- Pascal
- NetID
- Server- och nätverksinfrastruktur (som stödjer de NIS-systemen)
- Styr- och övervakningssystem (för de olika NIS-systemen)



I skede 1 ska anmälan rapporteras av incidentmottagaren och i skede 2 och 3 ska anmälan rapporteras av åtgärdsansvarig med hjälp av MSB:s verktyg, iron.msb.se.

Formulär och vägledning finns på MSB:s hemsida: msb.se

Rapportering av incident enligt säkerhetsskyddslagen

En anmälan vid säkerhetshotande händelser och verksamhet ska skickas av incidentmottagare till Säkerhetspolisen skyndsamt (samma dag) om

- det finns skäl att anta att en säkerhetsskyddsklassificerad uppgift otillåtet har röjts,
- det inträffat en IT-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet
- verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet

Säkerhetsskyddsincidenter gäller främst system inom vattenproduktion och

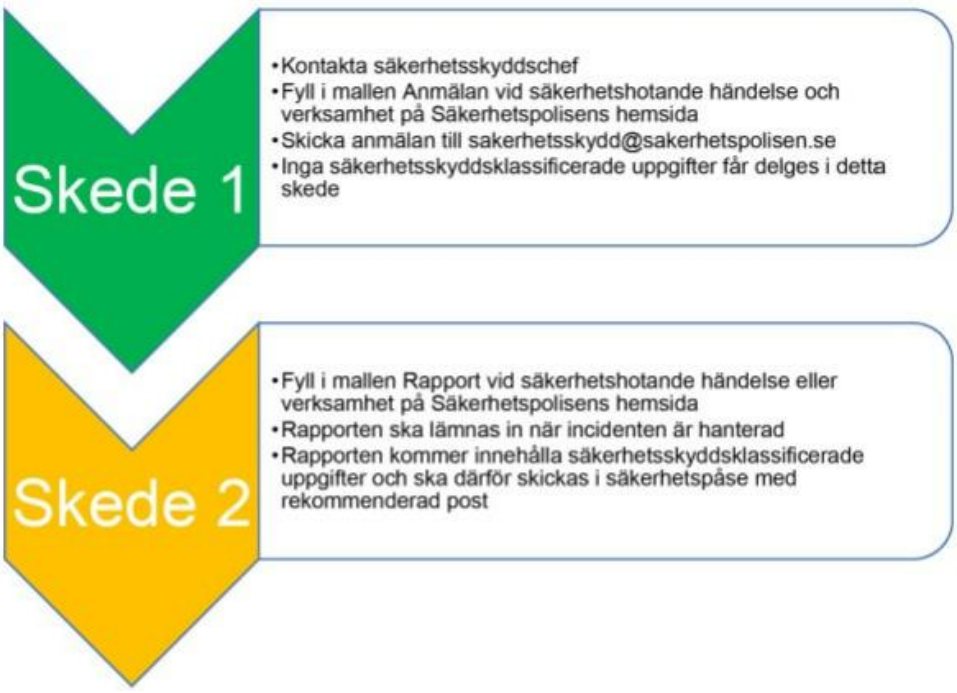
leverans, vissa fastighetstekniska system, signalskyddssystem samt härdade datorer. Kontakta säkerhetsskyddschef vid osäkerhet kring om en incident påverkar system eller uppgifter som omfattas av säkerhetsskyddslagen.

Åtgärdsansvarig ansvarar för att rapport för säkerhetshotande händelse eller verksamhet upprättas och skickas till Säkerhetspolisen. Notera att rapporten troligtvis kommer innehålla säkerhetsskyddsklassificerade uppgifter och ska behandlas i enlighet med styrdokumentet Tillämpningsanvisning för hantering av säkerhetsklassificerade uppgifter. Rapporten får under inga omständigheter skickas med e-post.

Formulär för incidentrapportering finns på Säkerhetspolisens hemsida och heter ”Anmälan vid säkerhetshotande händelser och verksamhet” (sakerhetspolisen.se).

Anmälan skickas till:
sakerhetsskydd@sakerhetspolisen.se

Säkerhetspolisens avdelning för säkerhetsskydd kan nås på detta telefonnummer:
010-568 70 00



Rapportering av incident enligt Dataskyddsförordningen

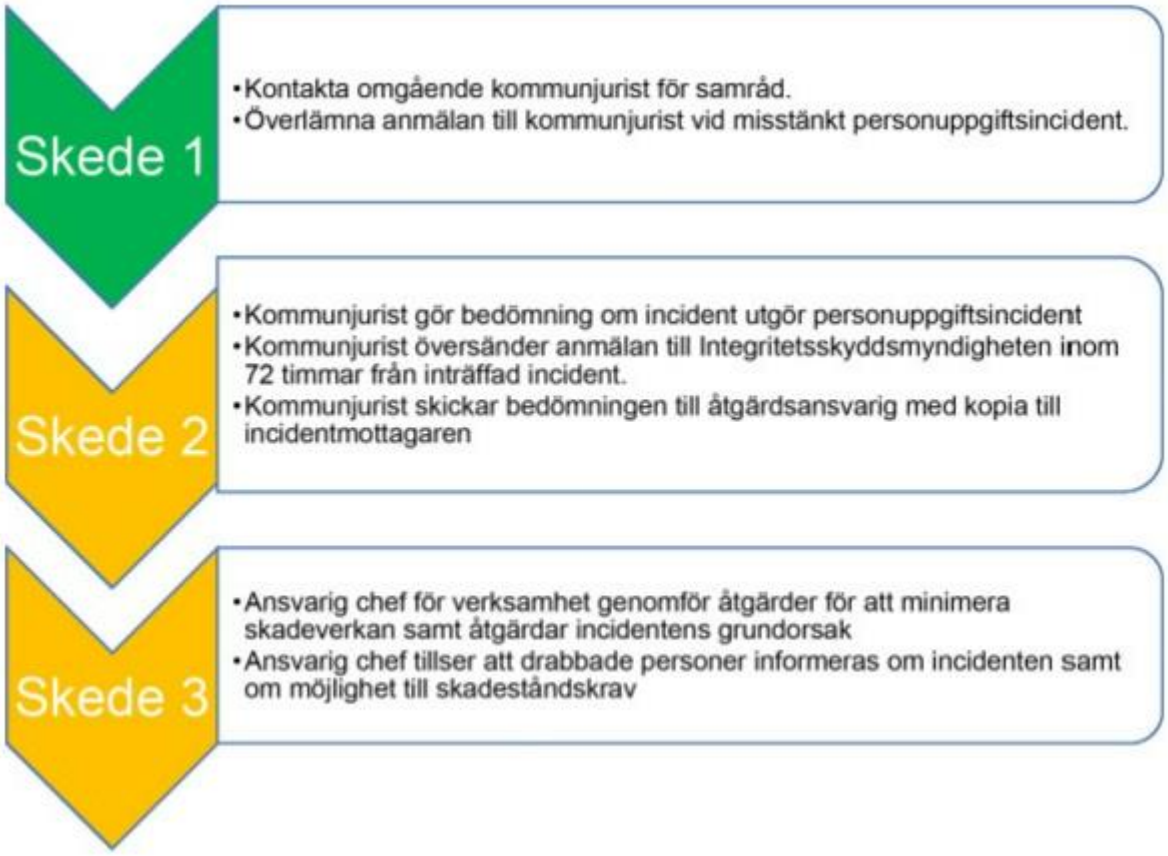
En personuppgiftsincident är en händelse som rör personuppgifter. Incidenten kan till exempel handla om att personuppgifter har blivit röjda för obehöriga, förstörda eller ändrade, gått förlorade eller kommit i orätta händer. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. Det kan exempelvis vara fråga om att personuppgifter som enligt dataskyddsförordningen anses vara känsliga, såsom etniskt ursprung, medlemskap i fackförening, uppgifter om hälsa, och som eventuellt även

omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400, OSL) har lämnats ut till fel person eller att personuppgifter i ett verksamhetssystem felaktigt raderats eller försvunnit på grund av ett tekniskt fel.

Anmälan till Integritetsskyddsmyndigheten ska göras inom 72 timmar från inträffad incident. Detta innebär att skede 1 och skede 2 måste genomföras skyndsamt.

Notera att en personuppgiftsincident som berör säkerhetsskydd inte ska rapporteras till kommunens jurister utan i stället till säkerhetsskyddschef för vidare hantering.

Åtgärdsansvarig tillser att drabbade informeras i den utsträckning detta följer av dataskyddsförordningen.



Skicka för åtgärd till åtgärdsansvarig

Åtgärdsansvarig för incidenter är chef för berörd verksamhet. Vid incidenter som påverkar mer än en enskild verksamhet inom samma sektor överförs åtgärdsansvaret till sektorchef. För incidenter i informationssystem som är kommunövergripande ansvarar respektive stabsenhetschef för åtgärdsansvaret. Om åtgärdsansvarig saknar befogenhet eller anser sig sakna kompetens att vidta åtgärder för kontinuitetshantering och återställande ska överordnad chef kontaktas. Ärendet eskaleras och åtgärdsansvar flyttas till högre chef. Vid mycket ansträngande bortfall av funktionalitet och kapacitet ska kommunens krisorganisation aktiveras genom tjänsteman i beredskap.

Det är viktigt att incidentmottagare överför dokumentation om redan vidtagna

åtgärder och upprättade kontakter till åtgärdsansvarig i samband med överlämnande, detta för att undvika dubbelarbete och för att undvika förvirring.

Följande frågor ska minst vara besvarade innan överlämning till åtgärdsansvarig, frågorna under varje punkt är tänkt som en hjälp att besvara huvudfrågorna och behöver inte vara besvarade:

- Vilka verksamheter påverkas och i vilken omfattning?
    - Gäller det enskilda medarbetare, enheter eller hel verksamhet?
    - Påverkas flera verksamheter?
- På vilket sätt påverkas verksamheten?
    - Föreligger fara för liv och hälsa?
    - Kan verksamheten bedrivas?
    - Kan verksamheten bedrivas fast med stora påfrestningar?
    - Kan vissa delar av verksamheten bedrivas?
    - Vilka funktioner i verksamheten påverkas?
- Redan vidtagna åtgärder?
    - Har teknisk support kontaktats?
    - Finns det någon tillfällig lösning som helt eller delvis kringgår problematiken?
    - Har chef i beredskap kontaktats?
    - Har extra personal kallats in?
    - Bedrivs verksamheten med alternativa metoder, exempelvis papper och penna eller annan typ av kontinuitetshantering?
    - Har någon annan verksamhet kontaktats?
- När rapporterades incidenten?
    - När rapporterades incidenten?
    - När upptäcktes incidenten?
    - När uppstod incidenten?
- Av vem rapporterades incidenten?
    - Av vem rapporterades incidenten?
    - Vem upptäckte incidenten?

Åtgärdsansvarig

Incident överlämnas och dokumentation fortsätter

Via stödsystemet lämnas ärendet över till den åtgärdsansvarige som dokumenterar eventuell ny information den får in.

Upprätta organisation

Den åtgärdsansvariga bör upprätta en organisation för att hantera verkningarna av uppkommen incident samt för återställande av normal drift. Ofta har

incidentmottagaren i ett tidigare skede upprättat kontakter både intern och externt som kan vara viktiga att vidmakthålla vid överlämning av incident. I dokumentationen från incidentmottagare bör framgå redan tidigare upprättade kontakter med exempelvis SOLTAK eller Kungälv energi.

En incidentorganisation kommer av bestå av olika funktioner beroende på incidentens art, omfattning och komplexitet. Nedan följer exempel på funktioner att beakta vid upprättande av incidentorganisation:

- **Systemförvaltare,** hanterar respektive informationstillgångar
- **Teknisk systemförvaltare (SOLTAK),** hanterar nätverks- och serverinfrastruktur
- **Jurist,** rättsliga förutsättningar
- **Registrator,** dokumentation
- **Dataskyddsombud,** rättsliga förutsättningar personuppgifter
- **Säkerhetsskyddschef,** vid säkerhetsskyddsincident
- **Säkerhetschef**
- **Informationssäkerhetssamordnare**
- **IT-strateg,** vid större incidenter som påverkar servrar, nätverk eller ett flertal system
- **Kontaktperson Kungälv energi,** vid kabelbrott, fjärrvärmeavbrott eller fiberproblematik
- **Kommunikatör,** kommunikation till verksamhet och drabbade kommuninvånare
- **Enhetschef/verksamhetschef** påverkad verksamhet, verkställa kontinuitetsplan för verksamheten tills incidenten är avhjälpt

Bedömning om kontinuitetshantering

Under den tid incidenten påverkar verksamheten kan det finnas behov av att aktivera kontinuitetshanteringsplaner. Vid en mindre incident kan verksamheten sannolikt fortsätta med ordinarie organisation och bemanning medan en större incident kan aktualisera förstärkt bemanning och alternativa arbetssätt.

Kontinuitetsplaner ska finnas upprättade för samtliga samhällsviktiga system och ska mildra verkningar av bortfall av funktionalitet i verksamhetssystem.

Eventuellt fortsatt rapportering enligt NIS-direktivet

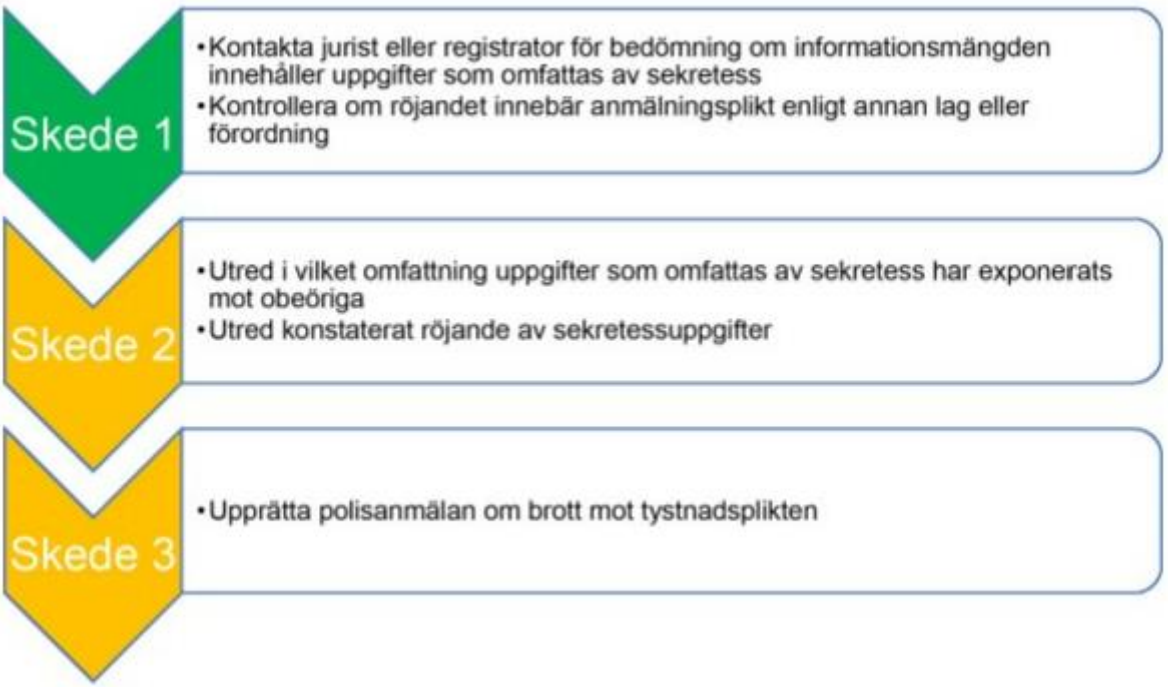
Om incidenten handlar om ett system som berörs av NIS-direktivet skall steg 2 genomföras inom 24 timmar efter upptäckt, steg 3 inom fyra veckor. De olika stegen registreras på MSB’s webbplats iron.msb.se.

Bedömning om sekretess röjts

Vid intrång eller felaktig uppsättning av informationssystem är det viktigt att utreda sannolikheten av att sekretess kommit obehörig till del. Bara det faktum att obehöriga kan ha tagit del av sekretess bör utredas, det behöver alltså inte handla om något konstaterat intrång i syfte att tillskansa sig uppgifter

som omfattas av sekretess. Bara det faktum att det funnits möjlighet för obehöriga att ta del av sekretessbelagda uppgifter ska hanteras som ett röjande.

Notera att en anmälan om brott mot tystnadsplikt bör upprättas oavsett om röjandet varit avsiktligt eller oavsiktligt.



Upprätta polisanmälan

Om det finns misstanke om att ett brott föreligger till exempel ett intrång i våra system, stöld av information, sabotage med mera skall en polisanmälan upprättas. Detta görs på polisens hemsida polisen.se utav åtgärdsansvarig.

Rapportera till säkerhetspolisen

Om en anmälan till säkerhetspolisen har skett tidigare ska en rapport (Rapport vid säkerhetshotande händelse eller verksamhet) sammanställas efter att incidenten är hanterad. Tänk på att hantera rapporten på korrekt sätt, den kan innehålla säkerhetsskyddsklassad information.

Upprätta grundorsaksanalys

Åtgärdsansvarig tillser att en grundorsaksanalys upprättas en tid efter att incidenten åtgärdats. Grundorsaksanalysen ska delges informationssäkerhetssamordnaren samt systemägare vid färdigställande.

Syftet med grundorsaksanalysen är att förstå vad som orsakat incidenten och vad som påverkat hur den utvecklats. 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.

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 stödmaterial.