Alf Jönsson
alf.jonsson@skane.se

INSTRUKTION

Datum: 2017-03-03 (2020-06-02)
Dnr: 1604654

Instruktion för hantering av informationssäkerhetshändelser- och incidenter

Syftet med instruktionen är att öka informationssäkerheten på så sätt att det ska finnas processer och metoder för att på ett strukturerat sätt klassificera och hantera informationssäkerhetsincidenter.

Målet är att undvika eller begränsa påverkan på verksamheten som direkt eller indirekt kan leda till skada.

Härmed beslutas att instruktion för hantering av informationssäkerhetshändelser- och incidenter fastställs

Alf Jönsson

Revisionshistorik

Datum	Ändring	Ansvarig
2017-02-23	Skapad	Johan Reuterhäll
2020-06-02	Rättning av benämning av kategorier, tillägg för SITHS-kort, uppdatering av bilaga 1 samt lagstiftning	Johan Reuterhäll

Koncernkontoret
Området för krisberedskap, säkerhet och miljöledning

Johan Reuterhäll
Informationssäkerhetschef
johan.reuterhall@skane.se

INSTRUKTION

Datum: 2020-06-02
Dnr: 1604654

Instruktion för hantering av informationssäkerhetshändelser- och incidenter

Bakgrund

Instruktionen har tagits fram med anledning av att det i de processer som finns för hantering av incidenter i dagsläget saknas metoder för klassificering av incidenter för att prioritera rätt. Denna instruktion slår bland annat fast vilka skalor och kriterier som ska gälla vid klassificering och prioritering av informationssäkerhetsincidenter. Instruktionen vägleder också på ett övergripande sätt vilka processer som ska finnas för att Region Skåne på ett effektivt sätt ska arbeta med hantering av informationssäkerhetsincidenter för att dels arbeta proaktivt och förebyggande dels hur inträffade incidenter ska hanteras och bidra till att de inte upprepas.

Syfte

Syftet med instruktionen är att öka informationssäkerheten på så sätt att det ska finnas processer och metoder för att på ett strukturerat sätt klassificera och hantera informationssäkerhetsincidenter.

Målgrupp

Målgrupp är alla medarbetare och externa leverantörer som hanterar Region Skånes information. Särskilt berörda är informationsägare, chefer, verksamhetsansvariga och systemansvariga, informationssäkerhetssamordnare och IT-säkerhetsansvariga. Även kravställare i upphandlingar av varor och tjänster som hanterar Region Skånes information är målgrupp för instruktionen.

Innehållsförteckning

Allmänt om informationssäkerhet

Information är en grundläggande byggsten i Region Skåne. En stor del av informationen omfattas av sekretess och har högt skyddsvärde. Det kan innebära stora negativa konsekvenser för Region Skåne om information går förlorad och inte finns tillhands när den behövs.
Informationen ska därför skyddas så att ingen obehörig får tillgång till den (konfidentialitet), att den är korrekt och inte är manipulerad eller förstörd (riktighet) och att den alltid finns när den behövs (tillgänglighet).

Styrande dokument och säkerhetsåtgärder garanterar inte skyddet av information, informationssystem, tjänster och infrastruktur. Även om säkerhetsåtgärder har blivit implementerade så återstår sårbarheter som försämrar informationssäkerheten och därmed gör informationssäkerhetsincidenter mer troliga. Det uppstår även nya hot och sårbarheter som tidigare inte identifierats.
Otillräckliga förberedelser för att hantera informationssäkerhetsincidenter kan innebära att tiden för att återgå till normalläge riskerar att bli längre och därmed drabbas verksamheten hårdare än vad som annars hade varit fallet.

Omfattning

Instruktionen omfattar Region Skånes alla informationstillgångar vilket inkluderar information oavsett om informationen behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö informationen förekommer.
Instruktionen gäller alla typer av informationssäkerhetsincidenter vilket även omfattar it-säkerhetsincidenter. Att ordet informationssäkerhetsincident används är för att syftet med denna instruktion är ökad *informationssäkerhet* och benämningen informationssäkerhetsincident träffar fler relevanta områden än vad benämningen it-säkerhetsincident gör.
Hantering av informationssäkerhetsincidenter ska regleras i avtal med externa leverantörer som hanterar Region Skånes information för att tillgodose Region Skånes informationssäkerhetskrav. Instruktionen utgör grunden för detta.
Avtal som tecknats med leverantörer innan instruktionen beslutats behöver inte justeras om det inte kan ske till rimlig kostnad. I det fall avtal omförhandlas eller förnyas gäller instruktionen.

Mål

Målet är att undvika eller begränsa påverkan på verksamheten som direkt eller indirekt kan leda till skada.

Region Skåne ska på ett strukturerat sätt:

a. proaktivt förebygga att informationssäkerhetshändelser uppkommer
b. upptäcka informationssäkerhetshändelser och hantera dessa effektivt, särskilt när det gäller händelser som kategoriserats som informationssäkerhetsincident

c. hantera och motverka negativa effekter av en informationssäkerhetsincident med rätt åtgärder och, när det behövs, med hjälp av krishanteringsplaner.
d. hantera rapporterade sårbarheter och
e. dra lärdomar av inträffade informationssäkerhetsincidenter-/händelser och rapporterade och åtgärdade sårbarheter

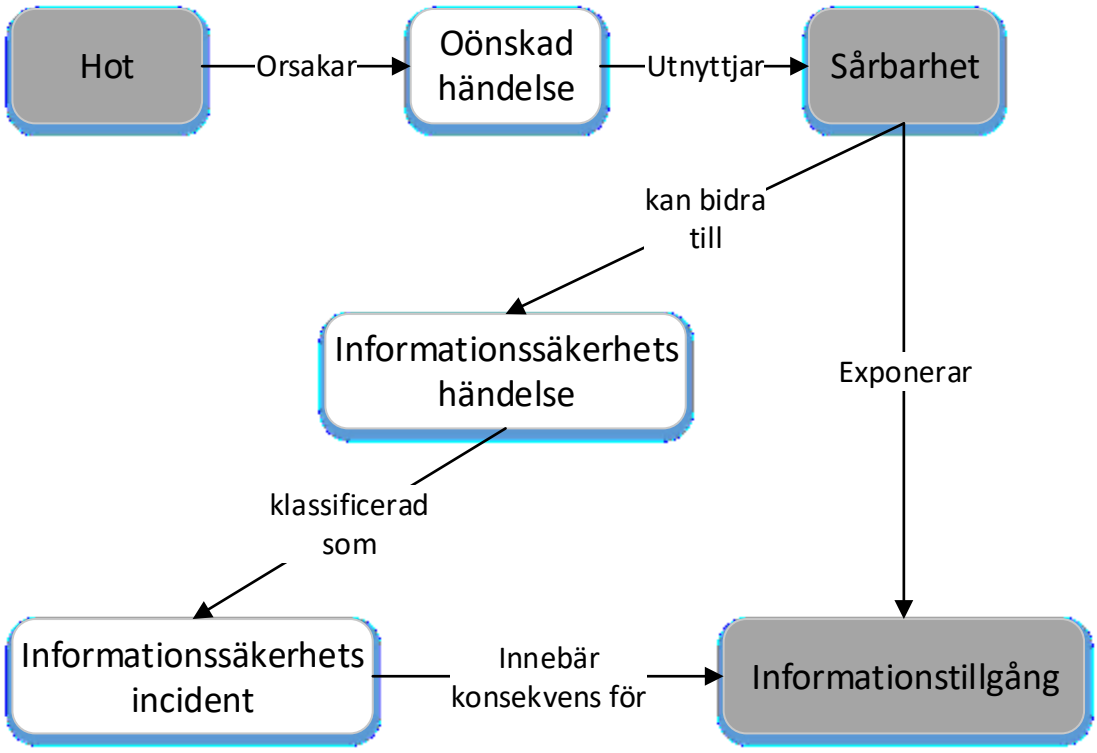
Region Skåne utgår från nedan standarder och ramverk i sin hantering av informationssäkerhetsincidenter:

- SS-ISO/IEC 27035:2012 (Informationsteknik – Säkerhetstekniker – Styrning och hantering av informationssäkerhetsincidenter och

- ITIL (Information Technology Infrastructure Library) som är ett ramverk med praktiska tillämpningar baserat på kraven i SS-ISO/IEC 20000 (IT Service Management).

Relationskarta

Nedan relationskarta visar hur olika delar relaterar till varandra.



Figur 1 - De skuggade objekten påverkas av de ofärgade objekten i kedjan som resulterar i en informationssäkerhetsincident

Hantering av informationssäkerhetshändelser

Hantering av informationssäkerhetshändelser sker enligt fyra huvudsakliga steg.

Steg 1: Detektering och rapportering av informationssäkerhetshändelse

Första fasen handlar om detektering och insamling av information om informationssäkerhetshändelser via personer eller automatiska funktioner. Region Skåne ska ha bevakning på förekomsten av sårbarheter som rör viktiga delar av infrastrukturen för att snabbt vidta åtgärder för att undvika informationssäkerhetsincidenter.

Detektering

Informationssäkerhetshändelser kan fångas upp av egen personal, en leverantör eller någon annan som upptäcker något som ger upphov till misstänksamhet. Det kan också vara händelser som fångats upp via automatisk analys av loggar från olika system, varningar från brandväggar, intrångsdetekteringssystem, antivirussystem m.m.

Sårbarheter

En sårbarhet är en brist i skyddet som kan utnyttjas. Sårbarheter finns i alla processer, all programvara och alla system. Vissa av dessa sårbarheter är kända och vissa är inte ännu kända. Kända sårbarheter kan ofta åtgärdas snabbt. Okända sårbarheter kan vara skadliga under en längre tid om de som utnyttjar dem känner till dem men inte de som har förmåga att åtgärda dem. När det gäller manuell hantering av information i exempelvis arkiv och posthantering finns också sårbarheter som kan utnyttjas eller som utan uppsåt kan medföra händelser och incidenter.
Vid upptäckt av sårbarhet ska en bedömning göras om sårbarheten är aktuell i något av Region Skånes system eller i någon motsvarande manuell process. Bedömning ska också göras hur sårbarheten ska klassificeras vilket utgör grund för prioritering av åtgärder.
Region Skåne ska, när det gäller IT-system, aktivt söka efter sårbarheter i de forum som finns tillgängliga och sträva efter att åtgärda dessa så snart det är möjligt.

Källor

Följande källor kan användas för att effektivt fånga upp förekomsten av informationssäkerhetshändelser och sårbarheter.

1. varningar från övervakningssystem så som exempelvis IDS/IDP, antivirusprogram, honungsfällor, logganalysprogram etc.
2. varningar från nätverksövervakningssystem så som brandväggar, flödesanalyser, webbfilter etc.
3. analyser av loggar tillhörande olika tjänster, servrar etc.
4. eskaleringar av händelser som inrapporterats av egen personal
5. eskaleringar av händelser som inrapporterats av supportpersonal
6. händelser rapporterade av användare

7. externa källor så som andra myndigheter, massmedia, nationella säkerhetstjänster, telekommunikationsföretag, outsourcade verksamheter, cert.se

Externa leverantörer
För att undvika sårbarheter ska det i avtal med externa leverantörer regleras hur säkerhetsuppdateringar och sårbarheter, som kan vara kritiska, ska hanteras. Utgångspunkten är att kritiska sårbarheter ska åtgärdas så snart det är möjligt. Om verksamheten påverkas av en åtgärd ska den underrättas om detta så att val av tidpunkt, om möjligt, kan anpassas.
Säkerhetsuppdateringar eller förändringar av processer och arbetssätt ska implementeras så snart det är möjligt.

Rapportering

Den person som blir uppmärksammad på en informationssäkerhetshändelse, som kan vara en incident, oavsett om det är genom egen observation, via automatiska övervakningsfunktioner eller på annat sätt, är ansvarig för att rapportera detta vidare till ansvariga via de processer som ska finnas för inrapportering av informationssäkerhetshändelser. Detta gäller såväl egen personal som den personal som Region Skåne anlitar eller tecknar avtal med.
Medarbetare och användare ska vara informerad om hur informationssäkerhetshändelser ska rapporteras och ha tillgång till gällande rutiner. Rutinerna kan behöva utformas olika beroende på verksamhet.

Innehåll i händelserapporten
Det ska finnas system för rapportering och hantering av informationssäkerhetshändelser.
Händelserapportering ska vara utformad så att rätt frågor ställs som behövs för att underlätta bedömningen om händelsen ska klassificeras som en incident eller inte. Det finns dock inget krav på att rapporten ska vara fullständig när den skickas in. Om det finns uppgifter i rapporten som inte är verifierad ska en notering kunna göras om det. Det är högre prioriterat att snabbt rapportera om en misstänkt eller inträffad händelse än att från början ha all information om det som inträffat. Rapporten byggs på med mer uppgifter efterhand. Det ska minst gå att se vad som hänt, när det hänt, vem som hanterat det och vilka beslut som fattats och av vem. Det ska gå att härleda rapporten till det aktuella systemet för att senare kunna göra sammanställningar över alla inträffade incidenter i ett visst system eller en viss process.

Externa leverantörer och konsulter
Externa leverantörer ska rapportera händelser och incidenter som rör de tjänster som levereras och den information som leverantören hanterar på uppdrag av Region Skåne. Rapportering ska ske så snart som möjligt efter att händelse eller incident inträffat.
I vissa fall har Region Skåne lagkrav att själv rapportera inom viss tid till tillsynsmyndighet. Underlag från leverantör ska i dessa fall skyndsamt levereras så att Region Skåne kan uppfylla de lagkrav som finns.

Om en extern leverantör hanterar någon del av organisationens informationstillgångar ska det finnas rutiner för hur leverantören ska kommunicera och samarbeta med organisationen kring incidenter.
Varje extern leverantör ska ha en utsedd kontakt (Single Point of Contact - SPOC) som Region Skåne kan vända sig till vid inträffade händelser eller incidenter. Kontakten ska, om behov finns, vara tillgänglig dygnet runt.

Externa leverantörer ska ha ett proaktivt arbetssätt vilket innebär att de själva och på eget initiativ ska informera om hot och sårbarheter samt lyfta förslag till förbättringsåtgärder med Region Skåne.
Krav på externa leverantörer och konsulter ska regleras genom avtal.

Säkerhetsskyddsklassificerade uppgifter
Sekretess gäller för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för Sveriges säkerhet om uppgiften röjs.
Händelser som misstänks röra Sveriges säkerhet ska omedelbart rapporteras direkt till säkerhetsskyddschefen. Kontakt tas via Region Skånes Tjänsteman i beredskap (RS TiB). Det kan även röra händelser som rör den tekniska infrastrukturen som har stor betydelse för Region Skånes förmåga att upprätthålla verksamheten och som har identifierats som säkerhetskänslig.
Vid informationssäkerhetshändelser som gäller säkerhetsskyddsklassificerad uppgift ska särskilda säkerhetsåtgärder vidtas så att inte säkerhetsskyddsklassificerade uppgifter lämnas ut av misstag eller avlyssnas i samband med rapportering och utredning.
Säkerhetsskyddschefen eller den säkerhetsskyddschefen utser leder utredningsarbetet i de delar som rör Sveriges säkerhet.
Säkerhetsskyddschefen ansvarar för att i vissa fall anmäla incidenter till Säkerhetspolisen[1].

Känsliga personuppgifter
Känsliga personuppgifter får inte hanteras i avvikelsehanteringssystem som inte är godkända för hantering av sådana uppgifter. Känsliga personuppgifter som exempelvis uppgifter om patienter ska, om uppgifterna behövs för handläggningen, i sådana fall hanteras separat och av behörig personal. Behörig är den som behöver uppgifterna för att kunna utföra sin arbetsuppgift. Rutiner ska finnas för hantering av känsliga personuppgifter i samband med en incident.

Vid misstanke om olovlig åtkomst till patientuppgifter
Misstanke om dataintrång kan uppstå vid en systematisk och regelbunden stickprovskontroll i verksamheten alternativt vid riktad kontroll. Riktad

[1] 2 kap. 10 § Säkerhetsskyddsförordningen (2018:658)

kontroll är specifik mot viss patient eller anställd och föranledd av misstanke om dataintrång t ex på grund av att en berömd person vårdats på enheten eller efter misstanke från patient.
Vid misstanke om olovlig åtkomst till patientuppgifter ska ärendet hanteras skyndsamt och i enlighet med gällande instruktion[2].

Bevisinsamling
Informationsinsamling om avvikande händelser är en förutsättning för ett framgångsrikt analysarbete, men informationen kan även komma att användas som bevismaterial. Om brott misstänks ska polisen kontaktas för polisanmälan och vidare instruktioner innan fortsatt arbete utförs för att inte riskera att förstöra bevismaterial. Undantag från kravet på instruktioner från polisen angående bevisinsamling kan göras om ett allvarligt läge måste åtgärdas. Det ska finnas rutiner för säkring av bevismaterial.

Steg 2: Bedömning och beslut

När informationssäkerhetshändelse rapporterats ska den bedömas om den utgör en informationssäkerhetsincident eller inte. Det ska ske med hjälp av den eller de händelserapporter som lämnats.
Bedömning ska göras om händelsen ska betraktas som möjlig eller bekräftad informationssäkerhetsincident och om eskalering behövs. Bedömningen ska utgå från en förutbestämd skala där det ingår att bedöma påverkan på verksamheten och om konfidentialitet, riktighet eller tillgänglighet till information påverkats. Med detta underlag ska bedömning göras om händelsen ska klassificeras som en informationssäkerhetsincident vilken prioritet den ska ha. Prioriteten avgör hur incidenten ska hanteras och vilka som ska informeras om incidenten. Incidentprioriteringsmatris finns nedan.

Händelser som inte kan bedömas och som det råder osäkerhet kring ska kunna eskaleras/överföras för bedömning hos den eller de som har kunskap att göra detta.
Loggning av beslut och händelser ska göras löpande eftersom de kan utgöra grund för kommande beslut och för senare uppföljning.

Om en incident kan bekräftas är målet att utreda följande så snart som möjligt:

a. Omfattningen av informationssäkerhetsincidenten, samt
   - hur den uppkom
   - vem eller vad som orsakade den,
   - tillgångar, infrastruktur, information, processer, tjänster eller tillämpningar som är påverkade eller som kan bli påverkade
   - effekt på Region Skånes kärnverksamhet
   - klassificering av den enligt beslutade skalor

[2] Instruktion – Dataintrång, åtgärder vid misstanke om olovlig åtkomst, daterad 2013-10-09

b. Om en incident orsakats av medveten mänsklig attack på ett informationssystem, tjänst eller nätverk så ska minst nedan ingå i utredningen:
   - hur långt in den som attackerat kommit och om denne har kontroll över något i nätverket och i så fall, över vad
   - vilken data som har varit åtkomlig för den som attackerat, vad som möjligen har kopierats, ändrats eller förstörts
   - vilken programvara som blivit kopierad, ändrad eller förstörd

c. direkta eller indirekta effekter av incidenten, exempelvis, finns det sårbarheter p.g.a. felaktigheter i programvara eller kommunikationsnät

d. hur informationssäkerhetsincidenten hanterats hittills

Incidenter som misstänks beröra informationens konfidentialitet eller riktighet ska omedelbart rapporteras till den eller de som är beroende av den information som påverkas eller påverkats.

Det ska finnas en fastställd rutin för hur incidenter i nationella tjänster ska hanteras inom organisationen. Vid incident som kan härledas till nationella tjänster ska hanteringen koordineras med den tjänstens fastställda incidentorganisation.

Steg 3: Hantering

Målet är att återgå till normalläge så snart som möjligt.

Omedelbara åtgärder

I flertalet incidenter kommer det behöva vidtas omedelbara åtgärder. Det kan handla om att koppla bort system, stänga ner system eller nätverk. Beroende på situation och hur incidenten klassificerats kan det krävas beslut på olika nivåer och att olika personer/funktioner informeras om det inträffade. Målet och den övergripande prioriteringen ska vara att minimera påverkan på verksamheten.
Behörighet att stänga ner hela eller delar av system och nätverk regleras genom delegationsordningen eller särskilt tilldelat förordnande.

Samverkan och samband med KSM

Hanteringen av större incidenter ska ske i samverkan med Området för krisberedskap, säkerhet och miljöledning (KSM) i enlighet med särskilt beslutade rutiner.

Incidenter som klassificeras som 1 och 2 enligt incidentprioriteringsmatrisen ska rapporteras till Region Skånes tjänsteman i beredskap (RS TiB). RS TiB ska lämnas möjlighet att följa ärendet. RS TiB kan överlämna ärendet till

annan person inom KSM som i så fall blir kontaktperson mot den som hanterar händelsen. I övrigt hanteras ärendet enligt den krishanteringsplan som finns.

Rapportering till myndighet

I det fall Region Skåne är skyldig att rapportera en incident till en tillsynsmyndighet så ska detta göras inom de tidsramar som lag eller förordning kräver.

Personuppgiftsincident

Rapportering till Datainspektionen ska vid personuppgiftsincidenter ske via dataskyddsorganisationen. Allt underlag som behövs i syfte att sammanställa rapport ska skyndsamt överlämnas till ansvarig för rapporteringen.

Incident enligt Lagen om informationssäkerhet i samhällsviktiga och digitala tjänster

Rapportering till tillsynsmyndigheten[3] via Myndigheten för samhällsskydd och beredskap (MSB) ska ske via de särskilt utsedda rapportörerna. Underlag som behövs för incidentrapporteringens olika faser ska vid begäran skyndsamt överlämnas till ansvarig rapportör.
Rutin för rapportering av NIS-incidenter finns framtagen av KSM.

Incident med digitala certifikat (SITHS)

Region Skåne är ansvarig utgivare av digitala certifikat (SITHS). Med det följer skyldighet att agera vid misstanke eller bekräftat missbruk av certifikat.
Vid en säkerhetsincident, dvs. misstanke om eller bekräftat missbruk av elektronisk identitetshandling ska Ansvarig utgivare se till att:

- Spärra de inblandade certifikaten
- Starta utredning om missbrukets omfattning
- Anmäla misstanke om eller bekräftat missbruk av certifikat till Inera.
- Upprätta incidentrapport

Polisanmälan

Om det finns anledning att tro att ett brott ligger bakom den uppkomna incidenten ska polisanmälan göras snarast. Polisanmälan görs i första hand av den verksamhet som har störst insikt i omfattning och orsak. Anmälare ska vara Region Skåne som juridisk person och som målsägare ska anges chefen för den verksamhet som i huvuddel äger de system, den utrustning eller de lokaler som påverkas. I undantagsfall kan KSM göra polisanmälan och stå som anmälare.
Polisanmälan bör inte innehålla information som är känslig eller sekretessbelagd och som kan ge angripare ledtrådar om sårbarheter.

---

[3] För hälso- och sjukvårdssektorn är det Inspektionen för vård och omsorg (IVO)

Anledningen är att polisanmälan och eventuell förundersökning är allmän handling.

Bedömning om incidenten är under kontroll

Efter att de omedelbara åtgärderna vidtagits ska en bedömning göras om incidenten är under kontroll. Om så är fallet ska åtgärder planeras för att återgå till normal verksamhet. Om det är möjligt ska information samlas in för att senare kunna utreda incidenten ytterligare.

Om informationens konfidentialitet och riktighet påverkats behöver ytterligare utredning göras av dessa informationsmängder för att kontrollera om sekretessbelagd information kommit obehöriga till del eller om information ändrats på något sätt. Observera att det redan i bedömningsskedet ingår att informera berörda om det misstänks att informationskrav på konfidentialitet eller riktighet påverkats.

Kommande/senare åtgärder

De aktiviteter som identifierats som nödvändiga att vidta ska tilldelas en ansvarig. Detta ska noteras i incidentrapporteringssystemet eller motsvarande och även följas upp där.
Vissa åtgärder syftar till att förhindra att incidenten återupprepas. Det kan exempelvis röra sig om en säkerhetsuppdatering som behöver installeras eller att en arbetsprocess som behöver förändras. Det kan också behövas bytas nycklar, certifikat, larmkoder, lösenord på system eller användarkonton eller slå av tjänster som inte ska vara igång.
Det bör övervägas om extra övervakning ska sättas in på berörda system för att upptäcka ovanliga eller misstänka händelser som kan tyda på fler informationssäkerhetsincidenter. Sådan övervakning kan också visa om fler system är påverkade av incidenten.

Utredning och forensiska analyser

Om det finns tecken som tyder på att informationssäkerhetsincidenten uppkommit genom ovarsamhet eller i brottsligt syfte ska detta utredas, antingen för att ge underlag till en intern utredning som kan utmynna i arbetsrättsliga åtgärder eller som underlag till polisutredning. Ofta finns dessa misstankar redan i ett tidigt skede och redan då ska bevis samlas in. Det är avgörande att bevisinsamling sker på rätt sätt. Om tid finns ska polis kontaktas för stöd. Det ska finnas särskilda rutiner för insamling av bevis.

Ansvarig för utredning är den förvaltning där incidenten inträffat. Driftorganisationen[4] kan även på eget initiativ genomföra utredning. Utredning kan även göras av KSM som ska ges åtkomst till den personal och den information som behövs för utredningens genomförande.

[4] Med driftorganisation avses systemägarnas driftsorganisation

Information och kommunikation

I vissa fall när en informationssäkerhetsincident inträffat behöver information lämnas ut till egna medarbetare och journalister. Det kan ske vid olika tidpunkter under arbetet, exempelvis när incidenten bekräftats, när den är under kontroll, när man beslutat om åtgärder, när den avslutats och vilka slutsatser man dragit.
Det ska finnas rutiner för vilka som ska informeras om vad och när. Samarbete ska etableras med ansvariga för mediakontakter.

Steg 4: Slutsatser och förbättringsåtgärder

Uppföljning av informationssäkerhetsincidenter ska ske enligt organisationens rutin och i två olika perspektiv:

- uppföljning av enskilda incidenter för att kartlägga bland annat orsak, förlopp och vilka eventuella ytterligare säkerhetsåtgärder som kan behövas för att förhindra att liknande incidenter inträffar,
- regelbunden uppföljning av samtliga incidenter för att urskilja eventuella mönster och systematiska felkällor för att kunna införa förbättringsåtgärder

Information till KSM

Utredningar som genomförs av inträffade incidenter ska delges KSM när de färdigställts. Det gäller även incidentrapporter och utredningar som tas fram av externa leverantörer som ett led i en leverans till Region Skåne. Utgångspunkten är att transparens ska råda. Sekretess eller handlingars status så som arbetshandling utgör inget hinder för överlämnande till KSM. I de fall informationen innehåller säkerhetsskyddsklassificerade[5] uppgifter ska mottagande tjänsteman vara säkerhetsprövad.

Utredningar som initieras av patientsäkerhetshändelse/-incident

Utredningarna sker när något inträffat eller hade kunnat inträffa och där man behöver utreda vilka brister som kan finnas i verksamheten och som kan påverka patientsäkerheten och hur dessa ska åtgärdas. Om det finns en koppling till informationssäkerhet ska informationssäkerhetschefen eller förvaltningens informationssäkerhetssamordnare kontaktas och om det är nödvändigt, lämnas möjlighet att delta i utredningen. Syftet är att sådana incidenter ska fångas upp och hanteras av rätt kompetens.

[5] Säkerhetsskyddsklassificerade uppgifter enligt definitionen i säkerhetsskyddslagen

Utlämnande av allmän handling

Rapporter om informationssäkerhetshändelser/ -incidenter kan utgöra allmän handling. Vid begäran om utlämnande ska sekretessprövning föregå ett eventuellt utlämnande.

Klassificering av incidenter

Hur en incident ska hanteras och prioriteras avgörs av vilka krav organisationen har på konfidentialitet, riktighet och tillgänglighet hos den eller de informationstillgångar som påverkas av incidenten. Kraven sätts när informationsklassificeringen genomförs. Om höga krav finns på konfidentialitet, riktighet och tillgänglighet finns och dessa inte går att upprätthålla så ska incidenthanteringen för att åtgärda incidenten ha motsvarande prioritet. För genomförande av informationsklassificering och vilka arbetsmetoder som ska användas finns särskilda instruktioner.

Påverkan (Impact)

Påverkan är ett mått på den effekt en incident har på verksamhetsprocesserna.
Följande skala ska användas för bedömning av en incidents påverkan.

Kategori	Påverkan
Mycket stor/ katastrof	• Samhällsviktiga och verksamhetskritiska funktioner påverkas eller, riskerar påverkas i stor omfattning. • Stor risk för allvarlig vårdskada föreligger alternativt, vårdskada har inträffat • Mycket stor eller, risk för mycket stor negativ effekt på verksamhetens/ Region Skånes förmåga att uppnå sina mål eller fullgöra sina primära uppgifter. • Mycket stor eller, risk för mycket stor skadekostnad för verksamheten/Region Skåne. • Mycket allvarlig/katastrofal, eller risk för mycket allvarlig/katastrofal förtroendeskada för verksamheten/Region Skåne. • Två eller flera system, med lägre tillgänglighetskrav, med en kumulativ påverkan som anses vara katastrofal/mycket allvarlig.
Betydande/ allvarlig	• Samhällsviktiga och verksamhetskritiska funktioner påverkas eller, riskerar påverkas i viss grad men är fortfarande tillgängliga med viss begränsning. • Risk för vårdskada föreligger • Betydande negativ effekt eller, risk för betydande negativ effekt på verksamhetens/ Region Skånes förmåga att uppnå sina mål eller fullgöra sina primära uppgifter. • Betydande skadekostnad eller, risk för betydande skadekostnad för verksamheten/Region Skåne. • Betydande/allvarlig eller, risk för betydande/allvarlig förtroendeskada för verksamheten/Region Skåne

	• Två eller flera system, med lägre tillgänglighetskrav, med en kumulativ påverkan som anses vara betydande /allvarlig.
Måttlig	• Viss negativ effekt eller, risk för viss negativ effekt på verksamhetens/ Region Skånes förmåga att uppnå sina mål eller fullgöra sina primära uppgifter. • Låg risk för vårdskada • Viss skadekostnad eller, risk för viss skadekostnad för verksamheten/Region Skåne. • Måttlig eller, risk för måttlig förtroendeskada för verksamheten/Region Skåne. • Två eller flera system, med lägre tillgänglighetskrav, med en kumulativ påverkan som anses vara måttlig.
Ingen/ försumbar	• Ingen eller försumbar negativ effekt på verksamhetens/Region Skånes förmåga att uppnå sina mål eller fullgöra sina primära uppgifter • Ingen risk för vårdskada föreligger • Ingen märkbar skadekostnad för verksamheten/ Region Skåne. • Ingen/försumbar förtroendeskada för verksamheten/Region Skåne.

Brådska (Urgency)

Brådska är ett mått på hur länge det dröjer tills en incident påverkar verksamheten betydligt.
Följande skala ska användas för att bedöma brådskan att avhjälpa en incident.

Kategori	Brådska
Kritisk	Förväntan på omedelbar eller mycket akut åtgärd • Tjänst är inte tillgänglig • Kritisk funktionalitet är inte tillgänglig • Påverkad verksamhet kan inte arbeta och det finns ingen reservplan/alternativ lösning • Oacceptabel prestanda • Skadan som incidenten orsakar ökar snabbt i omfattning.
Hög	Förväntan på snabb/akut åtgärd • Partiell förlust av funktionalitet, tjänster eller resurser • Intermittent störning/avbrott med hög frekvens • Komplex alternativ lösning • Skadan som incidenten orsakar ökar i omfattning.
Medel	Förväntan på skyndsam/snar åtgärd • Störningar på funktionalitet, tjänst eller resurser • Påverkad verksamhet är besvärad men kan fortfarande arbeta • Skadan som incidenten orsakar ökar inte i omfattning.
Låg	Förväntan på åtgärd inom rimlig väntetid

	• Mindre störning eller skönhetsfel på funktionalitet, tjänst eller resurser • Den berörda verksamhetens upplevelse kan eventuellt förbättras

Incidentprioriteringsmatris

Incidentprioriteringsmatrisen används för att visa vilken prioritet en inträffad incident ska få vilket styr inom vilken tid incidenten ska vara åtgärdad. Incidenter med stor påverkan och som är brådskande får högst prioritet medan incidenter som har liten påverkan och är mindre brådskande har lägre krav på åtgärdstider. Prioriteringsmatrisen används för varje enskild incident vilket kan innebära att olika incidenter i samma system kan prioriteras olika beroende på hur stor påverkan är samt hur brådskande det är. Kriterierna för detta anges ovan.

Koppling mellan riskmatris och incidentprioriteringsmatris

Incidentprioriteringsmatrisen har viss koppling till riskmatrisen. Riskmatrisen definieras i ”Instruktionen för riskhantering” och beskriver vilket riskvärde som identifierade risker har utifrån sannolikheten att risken inträffar och konsekvenserna. Risker med höga riskvärden behöver enligt den modellen åtgärdas antingen genom att minska sannolikheten att risken förverkligas vilket är det förebyggande/proaktiva arbetet eller genom att förbereda sig för att kunna omhänderta risker som realiserats i en incident vilket är det skadebegränsande/reaktiva arbetet.
Konsekvenserna är den gemensamma faktorn med den skillnaden att riskerna vid riskanalysen värderas utifrån sannolikheten att något inträffar och konsekvenserna av det inträffade. En redan inträffad händelse eller incident värderas utifrån påverkan på verksamhetens processer och med vilken brådska incidenten behöver åtgärdas där påverkan motsvarar konsekvenserna.

PRIORI-TERING		Påverkan - Impact			
		Mycket stor/ katastrof	Betydande/ allvarlig	Måttlig	Ingen/ Försumbar
Brådska - Urgency	Kritisk	1	2	3	3
	Hög	2	2	3	4
	Medel	2	3	3	4

	Låg	3	3	4	4

Beskrivning av incidentprioriteringsnivåer

Kategori	Brådska
Prioritet 1 (Kritisk)	Orsakar eller riskerar att orsaka väsentlig skada och olägenhet för Region Skånes verksamhet eller patientsäkerhet. Påverkar alla eller stor del av medarbetare i ett specifikt system eller funktion eller ställer ett väsentligt geografiskt område utan tillgång till systemstöd. Kan innebära stora ekonomiska konsekvenser för Region Skåne och Region Skånes kunder.
Prioritet 2 (Hög)	Orsakar olägenhet för Region Skånes verksamhet eller patientsäkerhet. Ett informationssystem är nere och det finns ingen dokumenterad lösning på felet. Incidenten påverkar en hel arbetsgrupp, avdelning (exempelvis en vårdcentral), ett stort antal slutanvändare eller viktiga funktioner.
Prioritet 3 (Medel)	En störande incident som inte påverkar Region Skånes verksamhet. Den har en operativ inverkan, men har ingen direkt inverkan på systemtillgänglighet. Det finns en dokumenterad lösning.
Prioritet 4 (Låg)	Har endast mycket liten eller ingen inverkan på Region Skånes verksamhet. Ingen direkt inverkan på medarbetares möjlighet att utföra sitt arbete.

Krav på avhjälpande åtgärder

Varje förvaltning ska, om det inte uppenbarligen är obehövligt, med hänsyn till det ansvar förvaltningen har för system och funktioner fastställa åtgärdstider som utgör grunden för de servicenivåavtal (SLA-avtal) som tecknas. Förutom åtgärdstider kan även andra krav ställas på exempelvis svarstider och servicetider. Tider ska sättas utifrån verksamhetens krav på tillgänglighet, de konsekvenser otillgänglighet leder till och de kostnader som följer. Åtgärdstiderna ska härledas till den incidentprioriteringsmatris som anges ovan och som gäller regionalt.

Andra skyddsåtgärder

Krav på konfidentialitet, tillgänglighet och riktighet kommer utifrån informationsklassificeringen. Dessa krav utmynnar inte endast i krav på leverantörer av IT-tjänster utan där finns ofta andra åtgärder som rör på fysiskt skydd, brandskydd, manuella reservrutiner, reservutrustning etc. Att enbart förlita sig på ett SLA-avtal och skyndsamma åtgärder för incidenthantering är inte alltid tillräckligt för verksamheter som har mycket höga krav på tillgänglighet.

Patientsäkerhet

Patientsäkerhet är mycket viktigt att upprätthålla för Region Skåne. Rätt prioritering av inträffade incidenter har direkt koppling till patientsäkerheten då framförallt tillgängligheten till system och riktigheten i information upphör, begränsas eller blir felaktig när incidenter inträffar. I bedömningskriterierna som anges ovan finns därför med bedömning av vårdskada. Om risk för vårdskada föreligger ska incidenten automatiskt prioriteras upp och hanteras med förtur framför andra incidenter med lägre prioritering.

SLA-avtal med leverantörer

Service Level Agreements (SLA) är ett avtal mellan en tjänsteleverantör och kund som beskriver vilken kvalitetsnivå en leverans ska ha. I SLA-avtal regleras bland annat vad som ska betraktas som fel och hur tillgänglighet ska beräknas. Avtalet kan även reglera vilken nivå tjänsten ska hålla i olika delar och i olika avseenden samt vilken tillgänglighet ett system ska ha under en tidsperiod samt vilka sanktioner som utgår om SLA-avtalet bryts i något avseende.

De SLA-avtal som Region Skåne tecknar med leverantörer av tjänster ska ta hänsyn till denna instruktion på så sätt att leverantören ska kunna åtgärda incidenter i enlighet med den prioritering en inträffat incident har.
I de fall leverantören ska bedöma prioriteringen av incidenter ska det göras enligt ovan beskrivna definitioner och prioriteringsmatris.

Problemhantering

Syftet med problemhantering är att förhindra problem och därmed uppkomst av incidenter, permanent lösa återkommande incidenter samt minimera påverkan i de fall incidenterna inte kan förhindras. Problemprocessen söker orsak till en eller flera incidenter och upprättar därefter ett åtgärdsförslag som genomförs.
Driftorganisationen för IT ansvarar för att närmare definiera hur processen för problemhantering definieras med utgångspunkt i denna instruktion och nedan problemklassificeringsmatris med koppling till incidentprioriteringsmatrisen.

Problemklassificering

Kategori	Påverkan
Kritisk	Problemet kan leda till en incident som prioriteras enligt nivå 1 i incidentprioriteringsmatrisen.
Hög	Problemet kan leda till en incident som prioriteras enligt nivå 2 i incidentprioriteringsmatrisen.
Medel	Problemet kan leda till en incident som prioriteras enligt nivå 3 i incidentprioriteringsmatrisen.
Låg	Problemet kan leda till en incident som prioriteras enligt nivå 4 i incidentprioriteringsmatrisen.

Bilaga 1 - Incidentkategorier

Följande kategorier ska användas vid kategorisering av incidenter. Huvudkategorierna är fasta men de exempel som anges under dessa kan utökas i den mån det behövs och är befogat.

Fysisk skada

Förlust av informationssäkerhet orsakas av avsiktliga eller oavsiktliga fysiska åtgärder. Det kan exempelvis röra sig om:

- Brand- eller vattenskador
- Manipulering och sabotage av utrustning
- Stöld av utrustning
- Förlust av utrustning, t.ex. borttappad dator, lagringsenhet (USB)

Fel i infrastruktur

Förlust av informationssäkerhet orsakas av fel i de bassystem och tjänster som ska stödja driften av informationssystem. Det kan exempelvis röra sig om:

- Strömavbrott
- Kylningssystem

Fel i nätverk

- Fel i komponenter i nätverk eller kablage som innebär avbrott
- Fel i nätverkstjänst (DNS, DHCP)

Hårdvarufel

- Felkonfigurationer
- Fel skapade av uppdateringar

Mjukvarufel

- Mjukvarufel som exempelvis bugg
- Handhavandefel

Tekniskt angrepp

Förlust av informationssäkerhet orsakas av att informationssystem angrips genom nätverk eller andra tekniska hjälpmedel. Angreppet sker genom sårbarheter i konfigurationer, protokoll eller program vilket resulterar i onormal status för informationssystemet eller potentiell skada för dess funktioner. Det kan exempelvis röra sig om:

- Internt angrepp
- Externt angrepp
- DoS-/DDoS- attacker

Brott mot lagstiftning eller interna regelverk

Förlust av informationssäkerhet orsakas av att det medvetet eller omedvetet sker brott mot lagstiftning eller interna regelverk. Det kan exempelvis röra sig om:

- Obehörig användning av resurser
- Brott mot upphovsrättslagen
- Otillåten spridning/lagring av information
- Användning av annans inloggningsuppgifter eller e-tjänstekort
- Användning av falsk identitet av patient eller kund
- Handhavandefel

Missbruk av funktioner

Förlust av informationssäkerhet orsakas av avsiktligt eller oavsiktligt missbruk av funktioner i informationssystem. Det kan exempelvis röra sig om:

- Missbruk av åtkomsträttigheter för att genomföra åtgärder som normalt sett inte ingår i arbetsuppgiften
- Vårdpersonal som tar del av patientjournaler trots att en vårdrelation saknas
- Nyttjandet av ”temp-admin” för att installera otillåtna programvaror

Skadlig kod

Förlust av informationssäkerhet orsakas av skadlig programvara eller skadlig kod. Det kan exempelvis röra sig om:

- Virus
- Trojan

Oönskad e-post

- Phishing
- Spam

Kompromettering av information

Förlust av informationssäkerhet orsakas av att informationen avsiktligt eller oavsiktligt utsätts för risk. Det kan exempelvis röras sig om:

- Avlyssning
- Social manipulation (social engineering)
- Stöld/förlust/manipulering av information
- Känslig information som blir publik

Bilaga 2 – Ordlista

Definitionerna är hämtade från SIS-TR 50:2015 – Terminologi för informationssäkerhet. Nedanstående definitioner är utdrag ur denna för vissa termer som förekommer i texten samt kompletterade.

KSM	Området för krisberedskap, säkerhet och miljöledning
ESM	Enheten för säkerhet och intern miljöledning
Hemlig uppgift/handling	Enligt offentlighets- och sekretesslagen 15 kap. § 2.
Hot	möjlig, oönskad **händelse** med negativa **konsekvens**er för verksamheten
Händelse	förekomst eller förändring av särskilda omständigheter
Konsekvens	resultat av en **händelse**
Informationssäkerhet	bevarande av **konfidentialitet**, **riktighet** och **tillgänglighet** hos **information** Informationssäkerhet ses som en uppsättning säkerhetsåtgärder för bevarande av egenskaper som **konfidentialitet**, **riktighet** och **tillgänglighet** men även **spårbarhet**, autenticitet, ansvarsskyldighet, oavvislighet och auktorisation. Informationssäkerhet omfattar områdena administrativ säkerhet och teknisk säkerhet.
Informationssäkerhetsincident	enskild eller flera oönskade eller oväntade informationssäkerhetshändelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet
Informationssäkerhetshändelse	bekräftad händelse som indikerar ett brott mot informationssäkerheten, styrande dokument eller annat som tidigare varit okänt som kan vara säkerhetsrelaterat
Informationstillgång	information, och resurser som hanterar den, som är av värde för en organisation

	Exempel på informationstillgångar är: - **information** (patientjournal, metodik, handling etc.) - **program** (applikation, operativsystem etc.) - **tjänster** (kommunikationstjänst, abonnemang etc.) - **fysiska tillgångar** (dator, data-medier, lokala nätverk etc.) - **personal** och deras kompetens, färdigheter och erfarenheter - immateriella tillgångar (rykte och image etc.) Informationstillgångar kan vara av fysisk eller logisk karaktär, eller bådadera.
Konfidentialitet	skydd mot obehörig insyn
Riktighet	skydd mot oönskad förändring
SLA	Service Level Agreements (SLA) är ett avtal mellan en tjänsteleverantör och kund som beskriver vilken kvalitetsnivå en leverans ska ha.
Tillgänglighet	åtkomst för behörig person vid rätt tillfälle
Spårbarhet	entydig härledning av utförda aktiviteter till en identifierad användare
Sårbarhet	brist i skyddet av en **tillgång** eller av en säkerhetsåtgärd som kan utnyttjas av ett eller flera **hot**
Tillgång	allt som är av värde för en organisation