Riktlinjer för hantering och rapportering av säkerhetsincidenter

1 Inledning

Karlstads universitet ska ha en ändamålsenlig process för hantering och rapportering av säkerhetsincidenter. Processen ska säkerställa myndighetens förmåga att skyndsamt upptäcka och bedöma incidenter, mildra effekter av incidenter, underlätta återgång till verksamhet på normal nivå, och förhindra upprepande av incidenter. Processen ska också fungera som ett stöd vid bedömningen om en inträffad säkerhetsincident ska rapporteras externt till MSB, Integritetsskyddsmyndigheten[1] eller Polismyndigheten.

En väl fungerande hantering av säkerhetsincidenter är en mycket viktig del av både det reaktiva och proaktiva säkerhetsarbetet. Det ger dels möjlighet att snabbt och effektivt agera på uppkomna hot och händelser, och dels möjlighet att i efterhand vidta förebyggande åtgärder för att motverka att liknande incidenter inträffar på nytt. En grundläggande förutsättning för att detta ska fungera är att samtliga verksamma vid Karlstads universitet har kunskap om vad som definieras som en incident, samt var och hur dessa ska anmälas internt inom organisationen.

Riktlinjerna beskriver på vilket sätt hantering och rapportering av säkerhetsincidenter ska ske vid Karlstads universitet, genom att bland annat fastställa de roller och funktioner som ansvarar för de olika delarna av incidenthanteringen.

2 Omfattning

Riktlinjerna omfattar alla incidenter som rör hantering av informationstillgångar (inklusive personuppgifter), fysiskt skydd (inklusive till exempel brandskydd), samt även incidenter inom medarbetarskydd (till exempel hot och våld samt stöld från medarbetare och studenter).

Riktlinjerna omfattar inte incidenter inom miljö- eller arbetsmiljöområdet. Sådana incidenter anmäls enligt särskilda rutiner, men kan även i vissa fall behöva utredas som en säkerhetsincident.

3 Definitioner

Definitionerna nedan kommer från SIS-TR 50:2015[2] eller SS-ISO/IEC 27000:2020 om inte annat uttryckligen anges.

---

[1] Den första januari 2021 bytte Datainspektionen namn till Integritetsskyddsmyndigheten (IMY).

[2] Termer, definitioner och förklaringar är återgivna ur SIS Tekniska rapport, Terminologi för informationssäkerhet, utgåva 1, med vederbörligt tillstånd från SIS Förlag AB.

Karlstads universitet
651 88 Karlstad
Tfn 054-700 10 00
Fax 054-700 14 60
Information@kau.se

Beslut:	111/21	Dnr:	C2021/962	Ersätter:	FB 11/16	Dnr:	C2016/276
Giltighet fr.o.m:	2021-11-15	t.o.m:	Tills vidare	Handläggare:	Niklas Nikitin		

Fysisk säkerhet: tekniska säkerhetsåtgärder relaterade till skydd av personer, lokaler och utrustning av betydelse för informationssäkerheten. Fysisk säkerhet är också ett eget säkerhetsområde som inte enbart relaterar till informationssäkerhet.

Hot: möjlig, oönskad händelse med negativa konsekvenser för verksamheten.

Incident: enskild eller flera oönskade eller oväntade händelser som har negativa konsekvenser för verksamheten.

Informationssäkerhet: bevarandet av konfidentialitet, riktighet och tillgänglighet hos information.

Informationssäkerhetsincident: enskild eller flera oönskade eller oväntade informationssäkerhetshändelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet.

IRT (Incident Response Team): organisatorisk funktion med uppgift att samordna aktiviteter i samband med incidenter.

IT-säkerhet: IT-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet.

Säkerhetsåtgärder: identifierad uppsättning åtgärder för att möta en organisations risker.

Sårbarhet: brist i skyddet av en tillgång eller av en säkerhetsåtgärd som kan utnyttjas av ett eller flera hot.

Risk: en kombination av en händelses konsekvenser (inklusive ändrade omständigheter) och tillhörande sannolikhet för förekomst.

4 Indelning av säkerhetsincidenter

Säkerhetsincidenter indelas in i tre incidentkategorier.

4.1 IT-incident

En IT-incident sker genom att till exempel obehöriga får tillgång till digital handlingar eller annan digital information, samt förlust eller annan åverkan på digital handlingar eller annan digital information. Några exempel på IT-incidenter är: datorvirus, bedrägeriförsök via e-post, datorhaveri som leder till förlorad information samt hackerangrepp på IT-system.

4.2 Fysisk säkerhetsincident

Fysiska säkerhetsincidenter sker genom att till exempel obehöriga får till tillgång till fysiska handlingar eller annan fysisk information, samt brand, förlust eller annan fysisk åverkan på fysiska handlingar eller annan fysisk information. Några exempel på fysiska incidenter är: stöld av pappersdokument samt avsiktlig eller oavsiktlig skadegörelse på originalhandlingar i form av pappersdokument.

Fysiska säkerhetsincidenter kan också innebära till exempel hot och våld mot anställda och studenter.

4.3 Personuppgiftsincident

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors rättigheter och friheter, till exempel om det finns risk för id-stöld, bedrägeri eller att känsliga personuppgifter röjs. En personuppgiftsincident kan till

exempel innebära att uppgifter om en eller flera registrerade har blivit förstörda, gått förlorade på annat sätt, eller kommit i orätta händer. Det spelar ingen roll om det har skett oavsiktligt eller avsiktligt.

5 Krav på rapportering från MSB

Enligt MSB:s föreskrift MSBFS 2020:8 är Karlstads universitet skyldig att rapportera en IT-incident till MSB som:

1. påverkat riktigheten, tillgängligheten eller konfidentialiteten hos den information som bedömts ha behov av utökat skydd[3], eller
2. inneburit att informationssystem som behandlar information som bedömts ha behov av utökat skydd inte kunnat upprätthålla avsedd funktionalitet, eller
3. påverkat myndighetens förmåga att utföra sitt uppdrag, eller
4. i övrigt allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten tillhandahåller åt en annan organisation.

Enlig MSB:s föreskrifter ska incidenter rapporteras skyndsamt, dock senast sex timmar från det att myndigheten har identifierat att en IT-incident omfattas av rapporteringsskyldighet, lämna en övergripande beskrivning (notifiering) av vad som inträffat. Sedan inom fyra veckor från det att universitet har identifierat att en IT-incident omfattas av rapporteringsskyldighet lämna en slutrapport.

6 Krav på rapportering enligt GDPR

Personuppgiftsincidenter som inträffas när Karlstads universitet är personuppgiftsansvarig ska rapporteras av universitet till Integritetsskyddsmyndigheten såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Rapporteringen ska ske utan onödigt dröjsmål, dock inte senare än 72 timmar efter att universitet har fått vetskap om personuppgiftsincidenten.

Karlstads universitet ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits (artikel 33 GDPR). Dokumentationsskyldigheten gäller även incidenter som inte behöver rapporteras till Integritetsskyddsmyndigheten.

7 Incidenthantering av säkerhetsincidenter

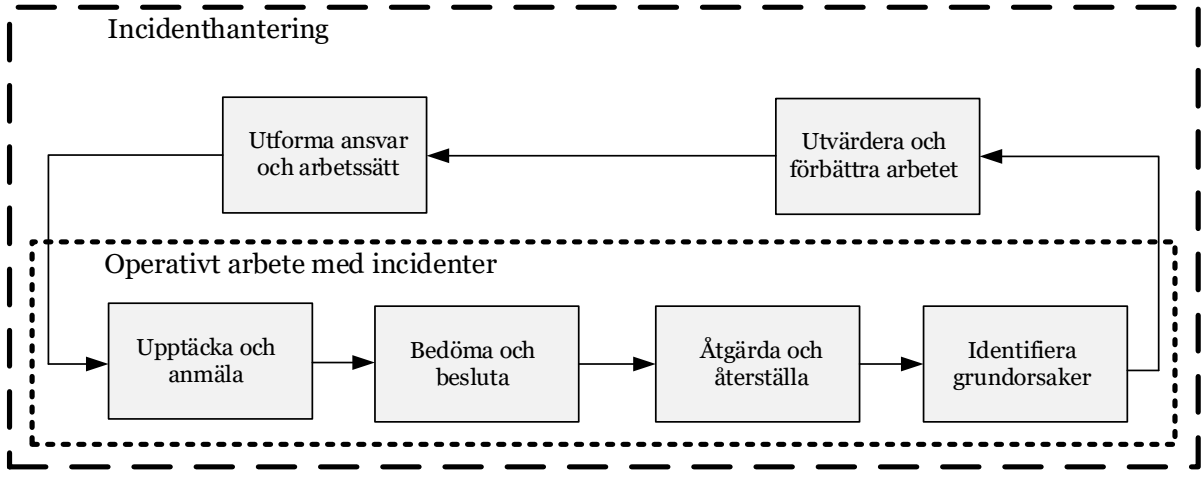
Incidenter kan vara av mycket olika karaktär och nivå. Det är därför viktigt att det finns uppgjorda strukturer för att hantera olika typer av incidenter. Till detta ska organisatoriska förutsättningar för hantering av incidenter kopplas. I detta ingår också att det ska finnas en planläggning och organisation för eskalering av hanteringen av incidenter.

Incidenten åtgärdas utifrån allvarlighetsgrad, med stöd av framtagna instruktioner, och med de resurser som är lämpliga för att minimera incidentens negativa konsekvenser.

---

[3] Med information som bedömts ha behov av utökat skydd avses information som enligt Karlstads universitets informationsklassningsmodell har bedömts behöva mer skydd än basnivå.

I incidenthantering ingår både det arbete som organisationen behöver göra för att utforma och förbättra det operativa arbetet med incidenter och det operativa arbetet i sig, se Figur 1.



Figur 1, Från MSB:s metodstöd för informationssäkerhet[4], bilden visar på incidenthanteringens olika delar.

7.1 Upptäcka och anmäla

Säkerhetsincidenter, ska snarast möjligt anmälas av den eller de som upptäckt eller fått vetskap om incidenten, se incidentanmälare, punkt 10.1.1 nedan. Incidenter kan upptäckas genom individuella observationer eller automatiserade larmsystem.
Individuellt upptäckta incidenter rapporteras enligt internt fastställda rutiner.

För incidenter som upptäcks via automatiserade larmsystem kan stödsystem användas.

7.2 Bedöma och besluta

IRT-gruppen[5], som ansvarar för den initiala bedömningen av IT-incidenter och personuppgiftsincidenter, respektive säkerhetsfunktionen[6], som ansvarar för den initiala bedömningen av fysiska säkerhetsincidenter, ska skyndsamt göra en första analys av incidentens potentiella påverkan för att bedöma incidentens allvarlighetsgrad och hur incidenten ska prioriteras.

Följande ska beaktas vid den initiala bedömningen av allvarlighetsgraden på incidenten:

- *Omfattning*: Hur omfattande är incidentens påverkan på Karlstads universitets resurser, personellt eller materiellt alternativt hur omfattande kan en hotande incident bli om hotet förverkligas?
- *Konsekvens*: Vilka konsekvenser får incidenten för Karlstads universitets förmåga att lösa sin uppgift alternativt vilka konsekvenser kan en sårbarhet få om hotet förverkligas?
- *Sannolikhet för eskalering och upptrappning*: Hur stor är sannolikheten att incidenten trappas upp eller sprider sig?

---

4 https://www.informationssakerhet.se/

5 En IRT-grupp finns inrättad på Karlstads universitets IT-avdelning.

6 Universitets säkerhetsfunktion består av säkerhetskoordinatorn och säkerhetschefen.

Den initiala bedömningen ska användas för att prioritera incidenten, hur brådskande det är att åtgärda incidenten, vem som är ansvarig, och vilka resurser som ska användas. Det är viktigt att tänka på att den initiala bedömningen kan behöva ändras under utredningens gång om det framkommer ny information om incidentens allvarlighetsgrad. Detta innebär att eskalering och upptrappning av vilka resurser och på vilken nivå besluten ska fattas kan behöva göras.

Vid behov, exempelvis vid allvarliga säkerhetsincidenter, informerar IT-chefen, säkerhetschefen, informationssäkerhetsansvarig och/eller dataskyddsombudet direkt till Karlstads universitets ledning. Vilken funktion som ansvarar för rapportering till ledningen beror på incidentens art.

Incidentens allvarlighetsgrad ligger också till grund för om en incident behöver rapporteras externt. Alla incidenter ska bedömas enligt följande:

- *Rapporteringsskyldiga*: En incident som omfattas av kraven på rapporteringsskyldighet i enlighet med MSBFS 2020:8 respektive artikel 33 GDPR.
- *Ej rapporteringsskyldiga*: En incident som inte omfattas av kraven på rapporteringsskyldighet i enlighet med MSBFS 2020:8 respektive artikel 33 GDPR.

7.2.1 Sekretess

Information om incidenter som avslöjar brister som kan användas av obehöriga för att påverka informationshanteringen på Karlstads universitet samt informationen om att universitet har eller inte har haft en incident kan vara skyddad av sekretess i enlighet med 18 kap. 8 § offentlighets- och sekretesslagen (2009:400). Universitets jurister ger stöd i bedömningen om information rörande en incident ska skyddas av sekretess.

7.3 Åtgärda och återställa

När en incident har inträffat ska återställning till normalläge ske så snabbt som möjligt. Detta är grundläggande för att säkerställa Karlstads universitets leveransförmåga och ska ske på ett effektivt och strukturerat sätt. Den som är åtgärdsansvarig, se punkt 10.1.3 nedan, ansvarar för arbetet med att åtgärda incidenten och samordnar de aktiviteter som behöver göras för att normal funktion ska återställas.

7.4 Identifiera grundorsaker

När incidenten är över och normal verksamhet pågått en tid ska grundorsaken till incidenten identifieras.

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.

Om det inträffar en incident där grundorsaken redan är känd men bättre säkerhetsåtgärder inte hunnit införas behövs ingen ny utredning. Däremot ska incidenten noteras så att åtgärderna ska kunna prioriteras utifrån de incidenter som verkligen uppstår.

Den som är operativ incidentsamordnare, se punkt 10.1.2 nedan, ansvarar för att grundorsakerna till incidenten utreds.

7.5 Utvärdera och förbättra arbetet

Uppföljning av incidenter ska ske enligt två olika nivåer:

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

I båda fallen är huvudinriktningen att bedöma kort- och långsiktig påverkan på Karlstads universitets verksamhet. Rapporterna ska ses som underlag för säkerhetsarbetet i allmänhet och mer specifikt för Karlstads universitets kontinuitetsplanering. Även statistik över inträffade incidenter ska kunna tas fram bland annat för rapportering till Karlstads universitets ledning och styrelse.

Uppföljning och analys av säkerhetsincidenter ska göras på operativ och strategisk nivå. Detta görs av informationsägare, systemägare och teknikresursägare med stöd av informationssäkerhetsansvarig respektive dataskyddsombud. Ansvaret för att detta genomförs är incidentägaren, se punkt 10.1.4 nedan.

7.6 Utforma ansvar och arbetssätt

För att hanteringen av säkerhetsincidenter ska fungera operativt och kunna följas upp behöver ett antal tydliga funktioner eller roller och deras arbetsuppgifter definieras i incidenthanteringsorganisationen, se även punkt 10 nedan. Det är viktigt att roller, ansvar och mandat är tydliga för att organisationen ska klara av att hantera den pressade situation som en säkerhetsincident kan innebära.

Ansvaret för det övergripande och organisatoriska arbetet med incidenter och att alla sex stegen i incidenthanteringen fungerar som de ska är incidentsamordnaren, se punkt 10.1.5 nedan.

8 Rapportering av incidenter

De incidenter som har bedömts rapporteringsskyldiga ska rapporteras till MSB respektive Integritetsskyddsmyndigheten beroende på om det är en IT-incident eller en personuppgiftsincident.

8.1 Rapportering av IT-incidenter

IRT-gruppen ansvarar för notifikationen till MSB. I IRT-gruppens frånvaro ansvarar IT-chefen följt att informationssäkerhetsansvarig för notifikationen till MSB.

Informationssäkerhetsansvarig ansvarar för slutrapporten till MSB. I informationssäkerhetsansvariges frånvaro ansvarar IRT-gruppen följt av IT-chefen för slutrapporten till MSB.

8.2 Rapportering av personuppgiftsincidenter

Dataskyddsombudet ansvarar för rapporteringen till Integritetsskyddsmyndigheten. I dataskyddsombudets frånvaro är det

informationssäkerhetssansvarig följt av avdelningschefen för rektors kansli som ansvarar för rapporteringen av incidenterna.

9 Polisanmälan av incidenter

Incidenter som bedöms som brottsliga ska bevissäkras och utredas enligt fastställda rutiner. Utifrån en bedömning som görs i varje enskilt fall kan en incident också behöva polisanmälas. Det är säkerhetsfunktionen som ansvarar för polisanmälningar.

10 Ansvar och roller för hantering av säkerhetsincidenter

För att hanteringen av säkerhetsincidenter ska fungera operativt och kunna följas upp behöver ett antal tydliga funktioner eller roller och dess arbetsuppgifter definieras i incidenthanteringsorganisationen. Det är viktigt att roller, ansvar och mandat är tydliga för att organisationen ska klara av att hantera den pressade situation som en incident kan innebära.

10.1 Incidenthanteringsorganisation

I MSB:s metodstöd[7] för informationssäkerhetsarbetet finns det funktioner utpekade för incidenthanteringen.

10.1.1 Incidentanmälare

Den som upptäcker en incident och som ska anmäla detta. Incidentanmälare kan vara alla medarbetare, IT-support, IT-drift, samt extern aktör som exempelvis leverantör eller användare utanför organisationen.

10.1.2Incidentmottagare/Operativ incidentsamordnare

Tar emot, dokumenterar, bedömer och samordnar på ett övergripande sätt det operativa arbetet med incidenter. Säkerställer att incidenterna åtgärdas om de behövs. Ser till att grundorsaken till incidenten utreds. På Karlstads universitet har IRT-gruppen denna funktion för IT-incidenter och personuppgiftsincidenter, respektive säkerhetsfunktionen för fysiska säkerhetsincidenter.

10.1.3Åtgärdsansvarig

Ansvarar för att på ett systematiskt sätt återställa normal verksamhet. På Karlstads universitet har IT-chefen denna funktion för IT-incidenter, säkerhetschefen har denna funktion för fysiska säkerhetsincidenter, och den ansvarige för verksamheten där incidenten inträffar (incidentägaren) har denna funktion för personuppgiftsincidenter.

10.1.4Incidentägare

Ansvarig för en verksamhet där incidenten inträffar. Kan till exempel vara en informationsägare eller ansvarig för ett visst IT-system. Incidentägaren eller någon den utser bör vara primär kontaktperson till åtgärdsansvarig. Incidentägaren är också huvudansvarig för att se över och uppdatera rutiner, samt informera och utbilda personalen, för att säkerställa att liknande incidenter inte ska upprepas.

---

[7] https://www.informationssakerhet.se/

10.1.5Incidentsamordnare

Incidentsamordnaren ansvarar för det övergripande och organisatoriska arbetet med incidenter och att alla sex stegen i incidenthanteringen, se punkt 7 ovan, fungerar som de ska. På Karlstads universitet har säkerhetschefen denna funktion.

10.2 Informationssäkerhetsansvarig

Ger stöd vid utredning av informationssäkerhetsincidenter. Informationssäkerhetansvarig ansvarar för slutrapporten till MSB för rapporteringsskyldiga IT-incidenter.

Gör sammanställningar över informationssäkerhetsincidenter. Rapporterar vid behov och regelbundet till universitetsledningen samt årligen till universitetsstyrelsen.

10.3 Dataskyddsombudet

Ger stöd vid utredning av personuppgiftsincidenter. Dataskyddsombudet ansvarar för rapportering av rapporteringsskyldiga personuppgiftsincidenter till Integritetsskyddsmyndigheten.

Gör sammanställningar över personuppgiftsincidenter. Rapporterar vid behov och regelbundet till universitetsledningen samt årligen till universitetsstyrelsen.

10.4 Personuppgiftsbiträden och vid utkontrakterad informationshantering

Vid anlitande av personuppgiftsbiträde samt vid utkontrakterad informationshantering ska det i avtal säkerställas att incidenter rapporteras på sådant sätt att Karlstads universitet kan uppfylla kraven i MSBFS 2020:8 respektive artikel 33 GDPR.