Mittuniversitetet
MID SWEDEN UNIVERSITY

Handläggningsordning för incidenthantering

Publicerad: 2023-05-02

Beslutsfattare: Förvaltningschef Lotten Glans

Ansvarig funktion: Avdelningen för Infrastruktur

Handläggare: Helena Wallskog

Beslutsdatum: 2023-05-02

Giltighetstid: Tillsvidare

Senaste översyn: 2023-05-02

Sammanfattning: Dokumentet beskriver ramarna för Mittuniversitetets interna hantering av incidenter. Detaljerade processer och arbetssätt beskrivs i rutindokument.

Tidigare versioner: MIUN 2020/1414. 2020-11-03

Innehållsförteckning

Handläggningsordning för incidenthantering

1 Inledning

Handläggningsordningen för hantering av incidenter vänder sig till alla verksamma, medarbetare och studenter vid Mittuniversitetet. Det huvudsakliga syftet med denna handläggningsordning är att beskriva hur incidenter ska hanteras och hur rapportering av incidenter ska ske vid Mittuniversitetet.

1.1 Definition incidenter

1.1.1 Informationssäkerhetsincident

Informationssäkerhetsincidenter är händelser som påverkar, eller kan komma att påverka, säkerheten negativt för universitetets informationstillgångar. Den gemensamma nämnaren är att informationssäkerheten hotas genom till exempel obehörig åtkomst till information, olaglig hantering av data, felaktig information eller brist på tillgång till information. Inom området informationssäkerhetsincidenter ingår även personuppgiftsincidenter.

Definieras av Myndigheten för samhällsskydd och beredskap (MSB) som: "En incident där information i systemet eller nätverket, snarare än systemet eller nätverket, i sig, har påverkats."

Exempel på informationssäkerhetsincidenter är om din dator har utsatts för intrångsförsök eller om du har fått kränkande eller anstötande e-post. Likaså om du misstänker falsk e-post (s.k "phishing).

1.1.2 IT-incident

En IT-incident är en oönskad och oplanerad störning eller en försämring av kvaliteten i en tjänst som kan få eller har fått negativa konsekvenser för verksamheten, enskild individ eller tredje man. En IT-incident kan antingen bero på ett avsiktligt eller oavsiktligt agerande.

IT-incidenter kan vara störning i mjuk- eller hårdvara, störning i driftmiljö, informationsförlust eller informationsläckage. Det kan också vara säkerhetsbrist i en produkt, ett angrepp eller handhavandefel.

1.1.3 Fysisk- och eller miljöincident

En fysisk- och eller miljöincident är en otillåten fysisk påverkan och åtkomst till, skador på och störningar i tillgången till organisationens information och informationsbehandlingsresurser.

Exempel på incidenter kan vara brand, översvämning, inbrott, inbrottsförsök, stöld, stöldförsök.

1.1.4 Arbetsmiljöincident - Tillbud och arbetsskada

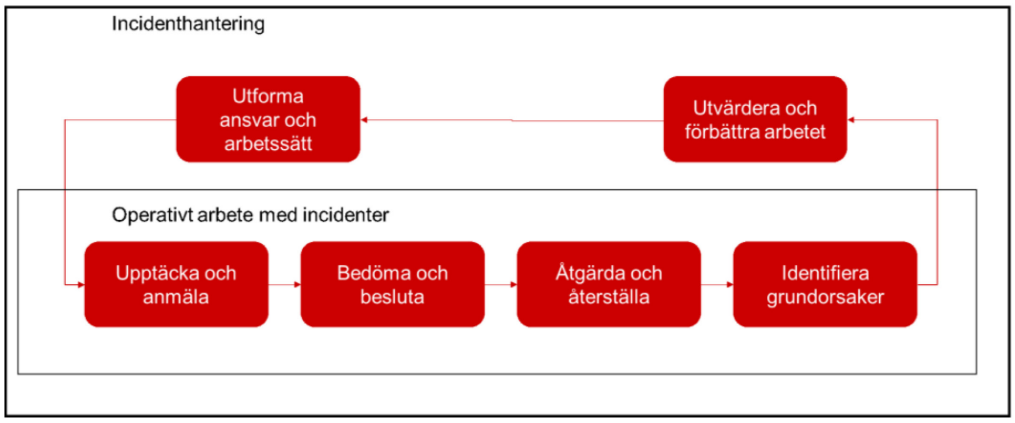
Ett tillbud är när något har inträffat som skulle ha kunnat leda till sjukdom eller olycksfall. En arbetsskada är olycksfall i arbetet, arbetssjukdom och färdolycksfall (resa till/från arbetet).

2 Processen

Syftet med incidenthantering är att:

- Synliggöra risker och vidta åtgärder efter att incidenter inträffat i verksamheten genom omedelbar hantering och skadebegränsning. (steg 1)
- Förebygga att liknande incidenter sker på nytt genom att analysera incidenter och vidta proaktiva åtgärder. (steg 2)

För att säkerställa att eventuella incidenter får minimal påverkan på universitetets verksamhet finns processer som visar hur hantering, rapportering och analys av incidenter ska genomföras.



Figur 1: Bilden visar på incidenthanteringens olika delar.

2.1 Hanteringen av incidenter:

2.1.1 Steg 1:

- begränsa incidenten
- identifiera och åtgärda relevanta orsaker
- rapportera incidenten enligt särskilda rutiner
- dokumentera information om incidenten innehållande, tidpunkt, vad som inträffat, omständigheter m.m.
- fastställa bevis genom exempelvis granskning av loggar
- rapportering av incident till Myndigheten för samhällsskydd och beredskap (MSB) respektive Integritetsskyddsmyndigheten (IMY) utifrån respektive myndighets fastställda direktiv, när detta är aktuellt.

2.1.2 Steg 2:

- efter att incidenten hanterats och åtgärdats ska en analys genomföras och dokumenteras:
    - ◊ o summering incident
    - ◊ o gjorda erfarenheter
    - ◊ o kortsiktig lösning

- ◊ o långsiktig lösning
- ◊ o uppdatering av rutiner, processer etcetera för att minimera risken för upprepad incident.

3 Rapportera incidenter

Den som upptäcker en incident vid Mittuniversitetet, ska omgående rapportera den.

Informationssäkerhetsincidenter, IT- incidenter samt fysiska och miljörelaterade incidenter kan rapporteras enligt något av följande sätt;

- Via serviceportalen
- E-post: itsupport@miun.se
- Telefon: 010-142 80 00, välj IT Support

Vid allvarligare informationssäkerhetsincidenter, IT-incidenter eller fysiska och miljörelaterade incidenter kontaktas IT Supporten alltid via ovanstående telefonnummer.

Arbetsmiljöincidenter: Rapporteringen görs av medarbetare/student via Mittuniversitetets incidentrapporteringssystem (IA). Händelser går också att rapportera via telefon genom att ladda ner IA som en app.

3.1 Incidentrapportering till Myndigheten för samhällsskydd och beredskap

3.1.1 Vilka incidenter ska rapporteras till MSB

En IT-incident som

- påverkat riktigheten, tillgängligheten eller konfidentialiteten hos den information som bedömts ha behov av utökat skydd, eller
- inneburit att informationssystem som behandlar information som bedömts ha behov av utökat skydd inte kunnat upprätthålla avsedd funktionalitet, eller
- påverkat myndighetens förmåga att utföra sitt uppdrag, eller

- i övrigt allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten tillhandahåller åt en annan organisation.

Bedömningen av om informationen är i behov av utökat skydd ska ske genom informationsklassning enligt 6 § p.1 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6)[1].

Myndigheten ska skyndsamt, dock senast sex timmar från det att myndigheten har identifierat att en IT-incident omfattas av rapporteringsskyldighet, lämna en övergripande beskrivning av vad som inträffat (notifiering).

Myndigheten ska inom fyra veckor från det att myndigheten identifierat att en IT-incident omfattas av rapporteringsskyldighet lämna följande uppgifter (slutrapportering).

1. Myndighetens namn.
2. En beskrivning av inträffad IT-incident, utifrån
   a) tidpunkt för när IT-incidenten inträffade och när den upptäcktes,
   b) tidpunkt för när drabbade informationssystem återgick till normaldrift,
   c) händelseförlopp,
   d) hanteringen av IT-incidenten, och
   e) typ, orsak och konsekvenser.
3. Vidtagna och planerade åtgärder med anledning av den inträffade IT-incidenten.

Om myndigheten inom ett år från det att slutrapportering har skett konstaterar att lämnade uppgifter är felaktiga ska uppgifterna korrigeras utan onödigt dröjsmål.

[1] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6)

Syftet med obligatorisk IT-incidentrapportering är enligt regeringen att stödja samhällets informationssäkerhet; det möjliggör en förbättrad lägesbild över informationssäkerheten, skapar förutsättningar för att vidta rätt skyddsåtgärder och utvecklar förmågan att förebygga, upptäcka och hantera IT-incidenter.

Genom att skyndsamt rapportera till Myndigheten för samhällsskydd och beredskap (MSB) för att därigenom få en samlad och övergripande bild, finns också möjlighet att samordnat vidta åtgärder för att avvärja eller begränsa konsekvenserna av allvarliga IT-incidenter. Om misstanke finns att ett brott har begåtts kommer en kontakt tas med rättsvårdande myndigheter efter dialog med ledningen.

Vid rapportering till Myndigheten för samhällsskydd och beredskap (MSB) ska en notifiering via telefon göras till MSB inom 6 timmar, därefter ska en slutrapport lämnas inom 4 veckor. Underlaget för slutrapporten finns på MSB:s hemsida.

3.1.2 Vem rapporterar till Myndigheten för samhällsskydd och beredskap, MSB?

Incidentkoordinator vid Infrastrukturavdelningen ansvarar för att rapportera IT-säkerhetsincidenter till Myndigheten för samhällsskydd och beredskap (MSB) enligt gällande regler.

3.1.3 Diarieföring och arkivering

Rapporterna och övriga handlingar i ärendet, exempelvis korrespondens med MSB bevaras och diarieförs och ges en sekretessmarkering i diariet.

3.2 Incidentrapportering till Integritetsskyddsmyndigheten

3.2.1 Vad är en personuppgiftsincident?

En personuppgiftsincident är en informationssäkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks.

Exempel:

- diskriminering
- identitetsstöld
- bedrägeri
- skadlig ryktesspridning
- finansiell förlust
- brott mot sekretess eller tystnadsplikt.

En personuppgiftsincident har till exempel inträffat när uppgifter om en eller flera registrerade personer har

- blivit förstörda
- gått förlorade på annat sätt
- kommit i orätta händer.

Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

Inom 72 timmar från det att man upptäckt en personuppgiftsincident ska den rapporteras till Integritetsskyddsmyndigheten. Anmälan behöver dock inte göras om det är osannolikt att incidenten leder till risker för enskildas fri- och rättigheter.

I vissa fall ska den registrerade informeras om incidenten.

Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten såvida inte någon av de i förordningen upptagna undantagen är aktuella.

Information till den registrerade krävs inte om något av följande villkor är uppfyllt:

a) Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder har tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.

b) Den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter sannolikt inte längre kommer att uppstå.

c) Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

Incidenten ska rapporteras via Integritetsskyddsmyndighetens e-tjänst och innehålla uppgifter om:

- vilken typ av incident det är fråga om
- vilka kategorier av personer som kan komma att beröras
- hur många personer det berör
- vilka konsekvenser incidenten kan få
- vilka åtgärder man vidtagit för att motverka eventuellt negativa konsekvenser.

3.2.2 Vem rapporterar till Integritetsskyddsmyndigheten?

Incidentkoordinator i samråd med dataskyddsombud rapporterar personuppgiftsincidenter, till Integritetsskyddsmyndigheten (IMY) enligt gällande regler.

3.2.3 Diarieföring och arkivering

Rapporterna och övriga handlingar i ärendet, till exempel korrespondens med Integritetsskyddsmyndigheten, bevaras och diarieförs och ges en sekretessmarkering i diariet.

4 Eskaleringsrutiner

Incidenter kategoriseras i 4 olika nivåer (låg, medel, hög och kritisk). Incidenter som kategoriseras som höga eskaleras till enhetschef för IT Drift & Utveckling. Incidenter som kategoriseras som kritiska eskaleras från enhetschef för IT Drift & Utveckling till avdelningschef för Infrastrukturavdelningen.

5 Utkontraktering

Om Mittuniversitetet överlåter en del av sin informationshantering till en aktör som inte omfattas av rapporteringsskyldighet ska Mittuniversitetet se till att aktören åtar sig att rapportera IT-incidenter till Mittuniversitetet på ett sådant sätt att Mittuniversitetet kan uppfylla kraven i Myndigheten för samhällsskydd och beredskap, MSB:s föreskrift 2020:8.

6 Ansvarsroller i processen

6.1 Verksamma

Verksamma vid Mittuniversitetet såväl studenter som medarbetare, rapporterar incidenter enligt denna handläggningsordning.

6.2 Chefer

Samtliga chefer ansvarar för att informera samtliga anställda om incidenthanteringsprocessen och vikten av att rapportera incidenter.

6.3 Systemansvariga

Systemansvariga ansvarar enligt systemförvaltningsmodellen att rapportera incidenter gällande verksamhetssystemen.

6.4 Ansvarsroller gällande Informationssäkerhetsincidenter, IT incidenter och fysiska- och miljörelaterade incidenter

6.4.1 IT Support

IT-supporten är en enhet inom Infrastrukturavdelningen och ansvarar för att:

- Ta emot och vidarebefordra inkomna incidenter till ansvarig i respektive underprocess.

6.4.2 Incidentkoordinator

Incidentkoordinator som är placerad på Infrastrukturavdelningen ansvarar för att:

- Samla in information
- Samordna nödvändiga resurser för att hantera incidenten
- Analysera incidenten
- Kommunicera till/med olika intressenter
- Eskalera incidenter
- Rapportera till MSB och IMY
- Vara kontaktfunktion mot MSB
- Retromöte genomförs och begär in nödvändiga handlingar

6.4.3 IT-säkerhetsspecialist

IT-säkerhetsspecialist som är placerad på Infrastrukturavdelningen ansvarar för att:

- Bevaka, analysera och utveckla incidentprocessen
- Rutiner för eskalering, larm och informationsspridning och andra processer kopplade till incidenthanteringen följs.
- Att handläggningsordningen är uppdaterad och aktuell

6.4.4 Dataskyddsombud

Dataskyddsombudet som är placerad på Universitetsledningens stab ansvarar för att:

- Stödja incidentkoordinatorerna i samband med rapportering av informationssäkerhetsincidenter som berör personuppgifter till Integritetsskyddsmyndigheten

6.4.5 Fastighet

Enheten fastighet som finns på Infrastrukturavdelningen ansvarar för att:

- Hantera incidenter som gäller fysisk- och miljörelaterad säkerhet.

6.5 Ansvarsroller gällande arbetsmiljöincidenter

HR-avdelningen finns som stöd för chefer i arbetet med att hantera inrapporterade arbetsmiljöincidenter.