Mittuniversitetet
MID SWEDEN UNIVERSITY

Handläggningsordning för incidenthantering

Publicerad: 2020-11-03

Beslutsfattare: Lotten Glans

Handläggare: Helena Wallskog

Beslutsdatum: 2020-11-03

Giltighetstid: Tillsvidare

Sammanfattning: Dokumentet beskriver ramarna för Mittuniversitetets interna hantering av incidenter. Detaljerade processer och arbetssätt beskrivs i rutindokument. Handläggningsordningen är anpassad utifrån Myndigheten för samhällsskydd och beredskaps föreskrifter MSBFS 2020:8.

Innehållsförteckning

1. INLEDNING 3
1.1 DEFINITION INCIDENTER 3
1.1.1 Tillbud och arbetsskada 3
1.1.2 Informationssäkerhetsincident 3
1.1.3 IT-incident 3
1.1.4 Fysisk- och eller miljöincident 3
2. PROCESSEN 3
2.1 HANTERINGEN AV INCIDENTER: 4
2.1.1 Steg 1: 4
2.1.2 Steg 2: 4
3. RAPPORTERA INCIDENTER 4
3.1 INCIDENTRAPPORTERING TILL MYNDIGHETEN FÖR SAMHÄLLSSKYDD OCH BEREDSKAP 5
3.1.1 Vad är en IT-incident? 5
3.1.2 Vilka incidenter ska rapporteras till Myndigheten för samhällsskydd och beredskap? 5
3.1.3 Vem rapporterar till Myndigheten för samhällsskydd och beredskap, MSB? 6
3.1.4 Diarieföring och arkivering 6
3.2 INCIDENTRAPPORTERING TILL DATAINSPEKTIONEN 6
3.2.1 Vad är en personuppgiftsincident? 6
3.2.2 Vem rapporterar till Datainspektionen? 7
3.2.3 Diarieföring och arkivering 7
4. UTKONTRAKTERING 7
5. ANSVARSROLLER I PROCESSEN 7
5.1 VERKSAMMA 7
5.2 TILLBUD 7
5.3 FYSISKA- OCH MILJÖINCIDENTER 8
5.4 INFORMATIONSSÄKERHETSGRUPP 8
5.5 IT-HELPDESK 8
5.6 SERVICECENTER 8
5.7 INCIDENTKOORDINATOR 8
5.8 DATASKYDDSOMBUD 8
5.9 KOMMUNIKATIONSAVDELNINGEN 8

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 Tillbud och arbetsskada

Ett tillbud är en händelse som hade kunnat leda till en skada, sjukdom eller ett olycksfall, men slutade väl. En arbetsskada är ett olycksfall i arbetet, färdolycksfall (resa till/från arbetet), en arbetssjukdom eller smitta.

1.1.2 Informationssäkerhetsincident

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

1.1.3 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.

1.1.4 Fysisk- och eller miljöincident

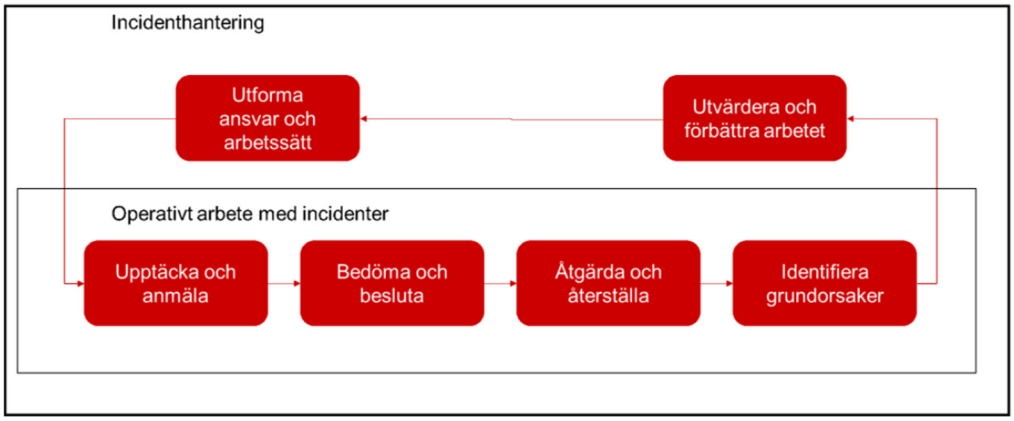
En fysisk- och eller miljöincident är en otillåten fysisk påverkan och åtkomst till, skador på och störningar i tillgången till organisationens information och informationsbehandlings-resurser.

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
- logga 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 Datainspektionen 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:
    - summering incident
    - gjorda erfarenheter
    - kortsiktig lösning
    - långsiktig lösning
    - uppdatering av rutiner, processer etc. för att minimera risken för upprepad incident

3. Rapportera incidenter

Den som upptäcker en incident vid Mittuniversitetet, ska omgående rapportera detta till:

E-post: kontakt@miun.se eller helpdesk@miun.se
Telefon: 010-142 80 00, IT-helpdesk
Fysiskt besök: IT-helpdesk eller Servicecenter
Vid allvarligare incidenter kontaktas IT-helpdesk alltid via ovanstående telefonnummer.

Tillbud: Rapportering av arbetsskada och tillbud är obligatorisk. Rapporteringen görs av medarbetare/student via Mittuniversitetets incidentrapporteringssystem (IA).

- Länk till IA-systemet, rapporteringskonto på webben för medarbetare
- Länk till IA-systemet, rapporteringskonto på webben för studenter

3.1 Incidentrapportering till Myndigheten för samhällsskydd och beredskap

3.1.1 Vad är en IT-incident?

En IT-incident karaktäriseras oftast av att det krävs någon form av omedelbar åtgärd för att hantera situationen och kan många gånger innebära en störning i förmågan att bedriva verksamheten eller att det kan påverka säkerheten för universitetets informationshantering. Några exempel på IT-incidenter kan vara kapad inloggning, dataintrång, angrepp med skadlig kod (virus) på dator, dataläckage, bedrägeriförsök via e-post eller säkerhetsbrist i produkt.

3.1.2 Vilka incidenter ska rapporteras till Myndigheten för samhällsskydd och beredskap?

Med IT-incidenter som omfattas av rapporteringsskyldighet menas en IT-incident som

1. påverkat riktigheten, tillgängligheten eller konfidentialiteten hos den information som bedömts ha behov av utökat skydd, 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.

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).

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.

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 ett formulär fyllas i för IT-incidenten och skickas in inom 6 timmar. Senaste versionen av dessa dokument går att hitta på MSB:s hemsida eller via nedanstående länk:

- IT-incidentrapportering för statliga myndigheter

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

Incidentkoordinator ansvarar för att rapportera IT-säkerhetsincidenter till Myndigheten för samhällsskydd och beredskap, MSB enligt gällande regler.

3.1.4 Diarieföring och arkivering

IT-incidenter rapporteras till Myndigheten för samhällsskydd och beredskap. Rapporterna och övriga handlingar i ärendet, t ex korrespondens med MSB bevaras och diarieförs och ges en sekretessmarkering i diariet.

3.2 Incidentrapportering till Datainspektionen

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 om 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.

3.2.2 Vem rapporterar till Datainspektionen?

Informationssäkerhetsgruppen och dataskyddsombud efter dialog med jurist ansvarar för att rapportera personuppgiftsincidenter, till Datainspektionen (DI) enligt gällande regler.

Inom 72 timmar från det att man upptäckt en personuppgiftsincident ska den rapporteras till Datainspektionen. 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.

Incidenten ska rapporteras via Datainspektionens 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

För dokumentation av personuppgiftsincidenter finns en framtagen mall (se Mall för dokumentation av personuppgiftsincidenter).

3.2.3 Diarieföring och arkivering

Personuppgiftsincidenter rapporteras till Datainspektionen. Rapporterna och övriga handlingar i ärendet, t ex korrespondens med Datainspektionen, bevaras och diarieförs och ges en sekretessmarkering i diariet.

4. 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.

5. Ansvarsroller i processen

5.1 Verksamma

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

5.2 Tillbud

Rapporteringen av arbetsskada och tillbud är obligatorisk och görs av medarbetare och studenter.

5.3 Fysiska- och miljöincidenter

Rapportering av fysiska och miljöincidenter görs av alla verksamma vid Mittuniversitetet och hanteras av fastighet inom avdelningen för infrastruktur.

5.4 Informationssäkerhetsgrupp

Informationssäkerhetsgruppen finns på avdelningen för infrastruktur, gruppen hanterar tillsammans med dataskyddsombudet informationssäkerhets- och personuppgiftsincidenter.

5.5 IT-Helpdesk

Tar emot och vidarebefordrar inkomna incidenter till ansvarig i respektive underprocess. Hanterar även IT-incidenter.

5.6 Servicecenter

Tar emot och vidarebefordrar inkomna incidenter till ansvarig i respektive underprocess.

5.7 Incidentkoordinator

Incidentkoordinator som är placerad på -avdelningen för infrastruktur loggar IT-incidenter, identifierar nödvändiga resurser för att hantera incidenten, samordnar och informerar nödvändiga intressenter samt säkerställer att slutanalys av incidenten efter slutförd åtgärd utförs.

5.8 Dataskyddsombud

Dataskyddsombudet ska bl. a informera och ge råd till medarbetare som handlar om deras skyldigheter enligt dataskyddsförordningen. Dataskyddsombudet ska även övervaka efterlevnaden av förordningen. Anmälningar av personuppgiftsincidenter till Datainspektionen bör ske i samråd med dataskyddsombudet som alltid ska informeras.

5.9 Kommunikationsavdelningen

Bistår vid behov med att informera intressenter.