Mittuniversitetet
MID SWEDEN UNIVERSITY

Handläggningsordning för incidenthantering inom IT och informationssäkerhet

Publicerad: 2026-06-16

Beslutsfattare: Avdelningschef Digitalisering och service Helena Wallskog

Ansvarig funktion: Digitalisering och service

Handläggare: Sofie Almqvist

Beslutsdatum: 2026-06-16

Giltighetstid: Tillsvidare

Senaste översyn: 2026-06-16

Sammanfattning: Handläggningsordningen reglerar ansvar, roller och arbetsprocesser för incidenthantering kopplat till IT och informationssäkerhet vid Mittuniversitetet. Handläggningsordningen är en del av ledningssystem för informationssäkerhet och syftar till att beskriva hur incidenter ska hanteras samt hur rapportering, uppföljning och förbättring ska ske.

Tidigare versioner: MIUN 2024/955, MIUN 2023/651, MIUN 2020/1414.

Innehållsförteckning

Handläggningsordning för incidenthantering inom IT och informationssäkerhet

1 Inledning

Handläggningsordningen för incidenthantering inom it och informationssäkerhet vänder sig till alla verksamma vid Mittuniversitetet, inklusive medarbetare och studenter. Syftet är att beskriva hur incidenter som påverkar eller riskerar att påverka universitetets information, digitala tjänster eller informationsbehandling ska hanteras samt hur rapportering, uppföljning och förbättring ska ske.

Handläggningsordningen är framtagen med utgångspunkt i Beredskapsförordningen 2022:524 samt Myndigheten för civilt försvars (MCF) föreskrifter. Vid hantering av personuppgiftsincidenter beaktas även gällande dataskyddsreglering (GDPR).

Dokumentet kompletteras av interna rutiner och instruktioner.

2 Definition av incidenter

2.1 Incident

En incident är en händelse som påverkar eller riskerar att påverka konfidentialiteten, riktigheten eller tillgängligheten hos universitetets information, informationsbehandling eller digitala tjänster.

Incidenter kan ha tekniska, organisatoriska eller fysiska orsaker, under förutsättning att de påverkar eller kan påverka informationssäkerheten eller universitetets digitala tjänster.

Exempel: driftstörning i system, intrångsförsök i dator eller nätverk, obehörig åtkomst till personuppgifter eller annan känslig information, misstänkt phishing, stöld eller förlust av informationsbärare, obehörig fysisk åtkomst till utrymmen där information eller informationssystem hanteras.

2.2 Allvarlig incident

En allvarlig incident är en incident som har orsakat eller bedöms kunna orsaka allvarlig påverkan på universitetets digitala tjänster, informationsbehandling eller informationssäkerhet, och som därför kräver samordnad hantering.

Vid bedömningen ska särskilt beaktas om incidenten medför eller riskerar att medföra allvarlig driftstörning, omfattande informationsförlust eller informationsläckage, eller betydande ekonomisk, rättslig eller förtroendemässig skada.

Exempel: personuppgiftsincident, ransomwareattack, omfattande systemavbrott, allvarligt dataintrång.

3 Roller och ansvar

3.1 Verksamma

Verksamma vid Mittuniversitetet, såväl medarbetare som studenter, ansvarar för att skyndsamt rapportera incidenter i enlighet med denna handläggningsordning.

3.2 Prefekter och avdelningschefer

Prefekter och avdelningschefer ansvarar för att säkerställa att medarbetare känner till incidenthanteringsprocessen och vikten av att rapportera incidenter.

Vid allvarliga incidenter ansvarar prefekter och avdelningschefer för att följa upp införandet och efterlevnaden av beslutade åtgärder inom den egna verksamheten.

3.3 Systemägare

Systemägare ansvarar för att säkerställa att beslutade säkerhetsåtgärder som föranletts av incidenter genomförs och följs upp för de system de ansvarar för.

3.4 Systemansvariga

Systemansvariga ansvarar för incidenter som rör de verksamhetssystem de förvaltar och ska samverka med Incident manager vid hantering av dessa.

I detta ingår att:

- rapportera incidenter som rör det egna verksamhetssystemet samt bidra med nödvändig systemkunskap vid analys och hantering,
- vid behov upprätthålla kontakt med systemleverantör,
- samverka med Incident manager avseende kommunikation som rör det aktuella systemet, samt
- eskalera till systemägare vid allvarliga incidenter.

Vid personuppgiftsincidenter medverkar systemansvariga i analys och rapportering till Integritetsskyddsmyndigheten (IMY).

3.5 IT Support

IT Support är en funktion inom Digitalisering och service som ansvarar för att ta emot rapporterade incidenter, göra en initial bedömning av incidentens art/kategori och omfattning samt hantera och åtgärda incidenter inom ramen för sitt uppdrag och mandat. Vid behov vidarebefordras incidenter till ansvarig funktion enligt fastställd process.

3.6 Incident manager

Incident manager, placerad vid Digitalisering och service, ansvarar för att samordna hanteringen av allvarliga incidenter. I detta ingår att:

- samla in och sammanställa relevant information,
- samordna nödvändiga resurser för hantering av incidenten,
- analysera incidenten och dess konsekvenser,
- kommunicera med berörda intressenter,
- eskalera incidenter enligt fastställda eskaleringsrutiner,
- ansvara för rapportering till Försvarets radioanstalt (FRA) och Integritetsskyddsmyndigheten (IMY) samt i särskilda fall anmälan till Polismyndigheten,
- fungera som kontaktfunktion mot berörda myndigheter,
- säkerställa att incidentrapport upprättas och dokumenteras, samt
- följa upp hanterade incidenter och vid behov initiera uppföljande möten med fokus på förbättring.

3.7 Incidenthanteringsteam

Vid allvarliga incidenter ska Incident manager kunna sammankalla ett incidenthanteringsteam för samordnad hantering av incidenten. Incidenthanteringsteamet består av relevanta representanter från berörda funktioner beroende på incidentens art och omfattning.

Incidenthanteringsteamet kan exempelvis inkludera representanter från:

- IT Drift och Utveckling
- IT Support
- Systemförvaltning
- Informationssäkerhet
- Dataskydd
- IT-säkerhet
- Fastighetsavdelningen
- Kommunikationsfunktion
- Berörd verksamhet
- Leverantörer

Incident manager ansvarar för att identifiera och sammankalla relevanta deltagare. Incidenthanteringsteamet ansvarar gemensamt för operativ samordning, lägesbild, prioritering av åtgärder samt informationsdelning under incidenthanteringen.

3.8 Beredskap

Beredskap är en funktion inom Digitalisering och service som hanterar larm från övervakade tjänster utanför ordinarie arbetstid. Vid larm som indikerar en incident ansvarar beredskap för att göra en initial bedömning, vidta nödvändiga inledande åtgärder samt eskalera vidare i enlighet med fastställda rutiner.

3.9 Dataskyddsombud

Dataskyddsombudet ansvarar för att, vid behov, delta i hantering och analys av personuppgiftsincidenter samt stödja incident manager vid rapportering av personuppgiftsincidenter till Integritetsskyddsmyndigheten (IMY).

3.10 Fastighetsavdelningen

Fastighetsavdelningen ansvarar för att hantera fysiska och miljörelaterade incidenter som påverkar IT och informationssäkerhet.

4 Incidentprocess

Incidentprocessen syftar till att säkerställa att incidenter hanteras skyndsamt och strukturerat för att begränsa konsekvenser, återställa verksamheten samt möjliggöra uppföljning och förbättring. Hantering av incidenter ska prioriteras i verksamheten.

4.1 Upptäck och rapportera

Den som upptäcker en incident vid Mittuniversitetet, ska omgående rapportera den enligt något av följande sätt;

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

Vid allvarliga incidenter kontaktas IT Support alltid via ovanstående telefonnummer.

4.2 Bedöma och klassificera

Rapporterade incidenter bedöms med avseende på omfattning och påverkan på verksamhet, information och digitala tjänster. Utifrån denna bedömning tilldelas incidenten en prioritet enligt fastställda prioritetsnivåer.

I detta steg bedöms även:

- om incidenten utgör en allvarlig incident,
- om incidenten omfattas av rapporteringsskyldighet till Försvarets radioanstalt (FRA) och/eller Integritetsskyddsmyndigheten (IMY), samt
- om incidenten kan innebära misstanke om brott och därmed ska polisanmälas.

4.3 Begränsa och åtgärda

Nödvändiga åtgärder ska vidtas för att begränsa incidentens konsekvenser. Åtgärder kan omfatta tekniska, organisatoriska eller fysiska insatser, exempelvis isolering av system, avstängning av konton eller andra skadebegränsande åtgärder.

4.4 Återställa

Efter att incidenten har begränsats ska drabbade tjänster och funktioner återställas till ordinarie drift i den mån det är möjligt. Återgång till normal verksamhet ska ske på ett kontrollerat sätt med hänsyn till säkerhet och verksamhetens behov.

4.5 Utvärdering och förbättring

Efter hantering av en incident ska den följas upp och analyseras i syfte att identifiera orsaker, dra lärdomar och vidta förbättringsåtgärder.

Vid behov ska uppföljande möten genomföras och rutiner, processer eller säkerhetsåtgärder uppdateras för att minska risken för att liknande incidenter inträffar igen.

Incidenthanteringsprocessen ska regelbundet övas för att säkerställa funktion, tydlig ansvarsfördelning och förmåga att hantera olika typer av incidenter. Lärdomar från genomförda övningar och inträffade incidenter ska systematiskt återföras till relevanta styrdokument, rutiner och arbetssätt.

5 Rapporteringsskyldiga incidenter

5.1 Incidentrapportering till Försvarets radioanstalt

Mittuniversitetet ska rapportera incidenter som enligt gällande regelverk omfattas av rapporteringsskyldighet till Försvarets radioanstalt (FRA). Bedömning av om en incident är rapporteringsskyldig till Försvarets radioanstalt (FRA) görs av Incident manager inom ramen för incidentprocessen. Rapportering ska ske skyndsamt i enlighet med gällande föreskrifters tidsangivelser.

5.2 Incidentrapportering till Integritetsskyddsmyndigheten

Personuppgiftsincidenter ska rapporteras till Integritetsskyddsmyndigheten (IMY) i de fall det krävs enligt gällande dataskyddsreglering (GDPR). Bedömning av om en incident är rapporteringsskyldig till Integritetsskyddsmyndigheten (IMY) görs av Incident manager, och vid behov, i samråd med dataskyddsombud.

5.3 Polisanmälan vid misstänkt brott

Incidenter som innefattar misstanke om brott ska polisanmälas. Ansvar för bedömning av om en incident ska polisanmälas samt för genomförande av polisanmälan följer den funktion som ansvarar för hanteringen av incidenten.

För incidenter som hanteras av Incident manager ansvarar Incident manager för bedömning och genomförande av polisanmälan. För incidenter som rör fysisk säkerhet ansvarar Fastighetschef för bedömning och genomförande av polisanmälan.

Bedömning sker vid behov i samråd mellan berörda funktioner.

5.4 Diarieföring och arkivering

Handlingar som rör rapportering till FRA, IMY och polismyndigheten ska diarieföras, bevaras och vid behov sekretessmarkeras i enlighet med gällande regler.

6 Eskaleringsrutiner

Incidenter eskaleras utifrån bedömd prioritet, omfattning och påverkan i enlighet med incidentprocessen.

Allvarliga incidenter eskaleras till enhetschef för IT Drift och Utveckling. Vid behov eskaleras ärendet vidare till avdelningschef för Digitalisering och service. Eskalering ska ske så snart incidenten bedömts vara allvarlig, eller tidigare om händelsen indikerar pågående skadlig aktivitet, omfattande driftpåverkan eller risk för informationsläckage.

Om en incident bedöms vara av sådan allvarlighetsgrad att krisledningen behöver aktiveras ska ärendet hanteras i enlighet med gällande handläggningsordning för krisorganisation.

7 Utkontraktering

Om Mittuniversitetet överlåter delar av sin informationshantering eller drift av nätverks- och informationssystem till extern part ska detta regleras genom krav så att Mittuniversitetet fortsatt kan uppfylla kraven på incidenthantering och incidentrapportering enligt gällande regelverk.

Avtal med externa parter ska innehålla krav på att incidenter som påverkar eller kan påverka universitetets information, informationsbehandling eller digitala tjänster skyndsamt rapporteras till Mittuniversitetet.

Mittuniversitetet ansvarar för bedömning, eskalering och eventuell rapportering till berörda myndigheter i enlighet med denna handläggningsordning.

8 Uppföljning och översyn

Digitalisering och service ansvarar för att denna handläggningsordning hålls aktuell samt för att vid behov initiera översyn och uppdatering av dokumentet.

Digitalisering och service ansvarar även för att följa upp och vidareutveckla incidenthanteringsprocessen, inklusive att identifiera förbättringsbehov med utgångspunkt i inträffade incidenter, genomförda uppföljningar och förändringar i gällande regelverk.

Översyn av handläggningsordningen ska ske minst vart tredje år eller vid behov, exempelvis vid förändringar i lagstiftning, föreskrifter eller organisation.