Mittuniversitetet
MID SWEDEN UNIVERSITY

Handläggningsordning för operativa IT-åtgärder vid incidenter

Publicerad: 2026-06-30

Beslutsfattare: Universitetsdirektör Louise Beskow

Ansvarig funktion: Digitalisering och service

Handläggare: Helena Wallskog

Beslutsdatum: 2026-06-30

Giltighetstid: Tillsvidare

Senaste översyn: 2026-06-30

Sammanfattning: Dokumentet beskriver ansvar, mandat och befogenheter för Digitalisering och service vid misstänkta eller konstaterade informationssäkerhetsincidenter och andra IT-relaterade incidenter. Det tydliggör vilka operativa åtgärder som får vidtas för att snabbt begränsa skada, skydda universitetets informationstillgångar och IT-miljö samt säkerställa dokumentation och uppföljning. Åtgärderna ska vara proportionerliga och genomföras med fokus på att stoppa incidenten, förhindra spridning och återställa verksamhetskritiska funktioner.

Tidigare versioner: MIUN 2024/2499

Innehållsförteckning

Handläggningsordning för operativa IT-åtgärder vid incidenter

Syfte

Syftet med denna handläggningsordning är att tydliggöra ansvar, mandat och befogenheter för Digitalisering och service vid hantering av informationssäkerhetsincidenter och andra IT-relaterade incidenter. Handläggningsordningen ska säkerställa att nödvändiga åtgärder kan genomföras skyndsamt för att begränsa påverkan på universitetets informationstillgångar, IT-tjänster och verksamhet.

Omfattning

Handläggningsordningen gäller vid misstänkta eller konstaterade incidenter som kan påverka konfidentialitet, riktighet eller tillgänglighet i universitetets informationstillgångar eller IT-miljö. Den omfattar såväl informationssäkerhetsincidenter som andra IT-relaterade händelser där tekniska åtgärder krävs för att begränsa eller förhindra skada på universitetets verksamhet. Exempel på sådana incidenter är skadlig kod, ransomware, phishing, kontokapningar, dataintrång, informationsläckage, obehörig åtkomst samt allvarliga driftstörningar med säkerhetspåverkan.

Ansvar och beslutsmandat

Digitalisering och service ansvarar för att bedöma incidentens omfattning och konsekvenser, vidta nödvändiga begränsande åtgärder samt dokumentera genomförda åtgärder. Ansvarig funktion ska även säkerställa att genomförda åtgärder kommuniceras enligt universitetets gällande process för incidenthantering.

Driftpersonal inom Digitalisering och service har mandat att besluta om och genomföra operativa åtgärder som krävs för att begränsa eller förhindra skada vid incidenter, när åtgärden bedöms vara nödvändig, proportionerlig och tidskritisk.

Vid mer övergripande eller verksamhetskritiska åtgärder, såsom åtgärder som påverkar större delar av verksamheten eller hela Mittuniversitetet (exempelvis avstängning av internet eller centrala tjänster), ska beslutet förankras hos Avdelningschef för Digitalisering och service. Om incidentens allvar, spridningsrisk eller tidskritikalitet kräver omedelbar åtgärd får beslut fattas utan föregående förankring, men ska då dokumenteras och skyndsamt rapporteras i efterhand.

Extern cybersäkerhetspartner får endast vidta åtgärder inom överenskommet mandat och enligt fastställda instruktioner. Åtgärder utanför detta ska eskaleras till Digitalisering och service.

Automatiserade åtgärder kan initieras genom säkerhetsövervakning eller andra tekniska skyddsfunktioner inom fastställda regler och mandat. De ska följa samma principer som manuella beslut, särskilt vad gäller proportionalitet, ändamålsenlighet och skydd av verksamheten. Åtgärderna ska dokumenteras och vid behov följas upp av ansvarig funktion inom Digitalisering och service.

Befogenheter att vidta operativa åtgärder

Befogenheterna omfattar de åtgärder som Digitalisering och service bedömer nödvändiga för att skydda universitetets informationstillgångar, användare, IT-tjänster och IT-infrastruktur vid misstänkta eller konstaterade incidenter. Åtgärder får vidtas utan föregående samtycke från berörd användare eller verksamhet när en fördröjning riskerar att förvärra incidentens konsekvenser eller öka risken för skada.

Konton och identiteter

Digitalisering och service får:

- Spärra eller stänga användarkonton.
- Tvinga lösenordsbyte.
- Återkalla aktiva inloggningssessioner.
- Inaktivera administrativa eller privilegierade behörigheter.
- Blockera autentisering till enskilda eller flera system.

Arbetsstationer och klienter

Digitalisering och service får:

- Isolera datorer från nätverket.
- Blockera nätverksåtkomst för klienter.
- Begränsa eller stänga åtkomst till interna IT-resurser.
- Begära att dator, mobiltelefon eller annan utrustning lämnas in för teknisk analys.
- Ominstallera eller återställa klientutrustning när detta bedöms nödvändigt för att eliminera säkerhetsrisker.
- Ta bort skadlig kod eller genomföra andra tekniska skyddsåtgärder.

Nätverk och kommunikation

Digitalisering och service får:

- Blockera eller begränsa internetanslutningar.
- Stänga av internetförbindelsen för hela eller delar av universitetet.
- Blockera nätverkssegment, IP-adresser, domäner eller protokoll.
- Begränsa eller stänga VPN-åtkomst.
- Isolera system eller nätverkszoner från övrig IT-miljö.

Servrar, system och tjänster

Digitalisering och service får:

- Stänga av eller begränsa IT-tjänster.
- Isolera servrar eller system från nätverket.
- Stoppa integrationer mellan system.
- Blockera åtkomst till lagringsytor och informationsresurser.
- Genomföra återställning av system eller information från säkerhetskopior.
- Genomföra andra nödvändiga tekniska åtgärder för att begränsa incidentens påverkan.

Analys och utredning

Digitalisering och service får:

- Samla in loggar och annan teknisk information.
- Genomföra teknisk felsökning och analys.

- Säkra digitalt bevismaterial.
- Anlita externt expertstöd efter beslut av behörig chef eller enligt gällande delegation.

Princip för genomförande

Åtgärder som vidtas med stöd av denna handläggningsordning ska vara proportionerliga i förhållande till incidentens omfattning och syfta till att:

1. Stoppa eller begränsa pågående incident.
2. Förhindra spridning.
3. Skydda informationstillgångar och IT-tjänster.
4. Säkerställa återställning av verksamhetskritiska funktioner.

Vid osäkerhet ska den åtgärd väljas som bedöms minska risken för ytterligare skada på universitetets verksamhet.

Dokumentation

Genomförda åtgärder ska dokumenteras i enlighet med universitetets process för incidenthantering. Dokumentationen ska, i den omfattning det är möjligt utifrån incidentens karaktär och allvarlighetsgrad, innehålla uppgifter om tidpunkt för åtgärden, vem som fattat beslut eller initierat åtgärden, vilken åtgärd som genomförts, orsaken till åtgärden samt vilka system, tjänster eller användare som berörts.

Uppföljning

Efter avslutad incident ska Digitalisering och service följa upp incidenthanteringen för att bedöma om de genomförda åtgärderna varit ändamålsenliga och om ytterligare säkerhetsåtgärder behöver införas. Uppföljningen ska även identifiera erfarenheter som kan bidra till förbättringar av processer, teknik, arbetssätt eller styrdokument för att minska risken för liknande incidenter i framtiden.