UMEÅ UNIVERSITET

ANVISNING FÖR HANTERING AV SÄKERHETSINCIDENTER

Typ av dokument:	Anvisning
Datum:	2026-11-06
Dnr:	FS 1.1-2135-26
Beslutad av:	Hans Wiklund
Giltighetstid:	Tillsvidare
Område:	Lokaler, it, miljö och säkerhet
Ansvarig förvaltningsenhet:	Enheten för juridik och informationsförvaltning
Ersätter dokument:	Nyinrättat

1 Inledning och syfte

Anvisningen vänder sig i första hand till de roller och funktioner som är involverade vid hantering av de säkerhetsincidenter som beskrivs i bilaga – Definition av säkerhetsincidenter.

Syftet med anvisningen är att skydda universitets skyddsvärda tillgångar vid säkerhetshändelser, att ge förutsättningar att upprätthålla verksamheten och säkerheten trots incidenter eller störningar samt att uppfylla lagstadgade krav på incidenthanteringen exempelvis genom cybersäkerhetslagen (2025:1506), beredskapsförordningen (2022:524), säkerhetsskyddslagen (2018:585) och GDPR.

Den första som får vetskap om en incident kan många gånger vara en enskild anställd, student, eller anknuten och det är därför samtidigt viktigt att samtliga verksamma vid universitet har kännedom om vad som utgör en incident och hur sådana händelser ska rapporteras.

Med en fungerande incidenthantering kan spridning av incidenter stoppas i tid, konsekvenser mildras och förebyggande åtgärder vidtas så framtida incidenter förhindras. För att kunna hantera incidenter på ett effektivt, ändamålsenligt och säkert sätt krävs tydlig ansvarsfördelning och ett strukturerat arbetssätt.

Anvisningen beskriver vad en säkerhetsincident är (bilaga), hur säkerhetsincidenter ska hanteras och dokumenteras, vilka ansvar och roller som finns i incidenthantering samt hur incidenter vid behov anmäls till andra myndigheter.

2. Process för hantering av säkerhetsincidenter

För att säkerställa att eventuella incidenter får minimal påverkan på universitetets verksamhet finns en process som beskriver flödet för rapportering, analys samt hantering.

2.1 Identifiera och rapportera säkerhetsincidenter

Säkerhetsincidenter kan identifieras på flera sätt.

När en avvikelse i normal verksamhet som kan föranleda en säkerhetsincident upptäcks ska detta rapporteras snarast möjligt. Hur rapportering ska ske ska framgå av medarbetarwebbens sidor ”Om något händer”, samt på motsvarande sidor riktade till studenter.

Om det gäller en säkerhetsskyddsincident (enligt definition i bilaga) ska det rapporteras via särskild rutin som beskrivs på sidan ’Säkerhetsskydd’ på medarbetarwebben.

Information om säkerhetsincidenter och hur dessa ska rapporteras ska ges i samband med utbildning av anställda och i information till studenter.

Andra källor till larm om säkerhetsincidenter är t ex driftsövervakningssystem av universitetsgemensamma IT-system och lokaler.

Snabb identifiering och rapportering av säkerhetshändelser är avgörande för att incidenthantering snabbt ska kunna påbörjas och även för att universitetet ska kunna uppfylla sina anmälningsskyldigheter till andra myndigheter, påverkade externa parter och privatpersoner inom gällande tidsramar. Vidarerapportering och informationsskyldighet beskrivs under avsnitt 4.

2.2 Hantera säkerhetsincidenter

Hur specifika incidenter ska hanteras i verksamheten ska beskrivas på sidorna ’Om något händer’ på medarbetarwebben. Övergripande ska incidenthanteringen ske enligt nedan:

2.2.1 Begränsa konsekvenser

Incidenter ska hanteras i prioritetsordning i relation till de konsekvenser som incidenten kan orsaka. Den ansvariga eller säkerhetsfunktion som tar emot incidenten gör en initial bedömning av allvarligheten.

Incidenthanteringsarbetet ska vara skyndsamt och aktivt för att minska spridning och begränsa konsekvenserna av det inträffade. Detta gäller alla typer av åtgärder såväl tekniska som administrativa. Med en god incidenthantering undviks att händelser utvecklas till kriser eller större avbrott i verksamheten.

2.2.2 Logga och analysera händelser

För att effektivt kunna begränsa och avbryta incidenter behöver information och bevis samlas in. Respektive ansvarig eller säkerhetsfunktion ska upprätta och föra en logg över händelser som relaterar till incidenten. För betydande eller allvarliga incidenter ska ’Mall för loggning’ på sidan ’Krishantering’ på medarbetarwebben användas. En löpande analys av händelserna ska också genomföras för att avgöra potentiell påverkan på information, individer och universitetets verksamhet. Denna löpande analys ska dokumenteras i loggen.

2.2.3 Samordna eller eskalera incidenthanteringen

Beroende av händelsetyp kan det finnas behov av samordnad incidenthantering mellan säkerhetsfunktioner eller eskalering i verksamheten. Hur eskalering ska ske vid olika typer av incidenter beskrivs under avsnitt 3 Roller och funktioner. Information ska även framgå i instruktioner på sidorna ’Om något händer’ på medarbetarwebben.

Vid eskalerad incidenthantering kan vid behov kontinuitets- eller krisplaner behöva aktiveras. Berörda säkerhetsfunktioner och eventuella krisgrupper ska få information så snart som möjligt.

2.2.4 Analysera och vidta åtgärder
Den inträffade incidenten ska analyseras för att synliggöra risker så att rätt åtgärder vidtas. Vid avbrott i verksamhet eller funktion ska sådan analys ske och nödvändiga åtgärder genomföras innan verksamhet eller funktion kan återställas.

2.2.5 Återställ verksamhet eller funktion
Efter vidtagna åtgärder och eventuella besiktningar kan verksamhet eller funktion återställas till normal nivå.

Återställning av påverkad information och funktionalitet i IT-system ska ske enligt systemets återställningsplan och universitets prioritetsordning.

2.3 Dokumentera och utvärdera efter hanterad säkerhetsincident
Den som är ansvarig för hanteringen av incidenten alternativt aktiverad krisgrupp ska, efter incidenter som varit betydande eller allvarliga, säkerställa och sammanställa dokumentationen över incidenthanteringens olika steg, samla in erfarenheter från delaktiga funktioner och roller samt analysera och utvärdera incidenten. Utvärderingen inklusive en analys av incidentens grundorsaker ska synliggöra lärdomar och belysa om arbetssätt och åtgärder haft avsedd effekt, men också om stöd finns i befintliga rutiner och arbetssätt. Efter genomförd utvärdering ska resultatet dokumenteras och förmedlas till berörda samt eventuella åtgärder genomföras, inklusive uppdatering av rutiner och arbetssätt, för att minska sannolikheten att incidenten återupprepas.

’Mall för utvärdering av betydande incident’ på sidan ’Krishantering’ på medarbetarwebben ska användas. En sammanställning av incidenthanteringen tillsammans med den sammanfattande utvärderingen och vilka åtgärder som planeras med anledning av den ska beskrivas.

2.4 Öva incidenthantering återkommande
Hantering av incidenter ska återkommande övas i verksamheten för att alla funktioner och involverade roller snabbt ska kunna agera om något händer. Incidenthantering övas med fördel samordnat med övningar av kris- och kontinuitetsplaner.

3. Roller och funktioner

Ansvarsfördelningen inom hantering av säkerhetsincidenter beskrivs i Regel för universitetsgemensamt säkerhetsarbete samt förtydligas nedan.

Enskild medarbetare eller student

En medarbetare som upptäcker en avvikelse i normal verksamhet som kan föranleda en säkerhetsincident har ett ansvar att rapportera detta så fort som möjligt enligt gällande rutiner (avsnitt 2.1)

En student som upptäcker motsvarande uppmanas också rapportera detta så fort som möjligt enligt universitets rutin.

Chef (Systemägare) oavsett nivå – t ex dekan, prefekt, enhetschef eller motsvarande

Ansvarar för att universitetets rapporteringsvägar för incidenter är kända i sin verksamhet och att incidenter rapporteras enligt gällande rutiner (avsnitt 2.1) samt att vid behov informera överordnad chef.

Chef ansvarar för hantering av säkerhetsincidenter i sin verksamhet, inklusive genomförande av åtgärder med stöd av respektive säkerhetsfunktion beroende på incidenttyp, samt att följa upp införandet och efterlevnaden av beslutade säkerhetsåtgärder som föranletts av en säkerhetsincident.

3.1 Stödjande och samordnade säkerhetsfunktioner

Vid behov av stöd från flera säkerhethetsfunktioner sker samordning mellan respektive säkerhetsfunktion.

IRT – teamet vid Enheten för IT-stöd och systemutveckling (ITS)

Incident response team, IRT ger råd och stöd vid cybersäkerhetsincidenter, dvs informationssäkerhets-, IT-säkerhets- och personuppgiftsincidenter, och arbetar aktivt med att förebygga, upptäcka och utreda cybersäkerhetsincidenter vid Umeå universitet.

IRT bedömer initial allvarlighetsgrad, analyserar och hanterar inkomna cybersäkerhetsincidenter samt involverar dataskyddsombud vid personuppgiftsincidenter.

IRT samordnar det operativa incidenthanteringsarbetet vid cybersäkerhetsincidenter och säkerställer att loggning av händelser under incidenthanteringen sker samt att universitetets interna kommunikationsbehov angående incidenthanteringen tillgodoses under incidenten. IRT ansvarar även för eventuell anmälan av cyberssäkerhetsincident till Nationellt cybersäkerhetscenter (NCSC).

IRT kan vid pågående incident fatta beslut om begränsande åtgärder i universitetets IT-miljö. Detta gäller såväl IT-tjänster som utrustning oavsett om de är centralt eller lokalt placerade vid universitet eller hos extern leverantör.

IRT har mandat att utifrån behov involvera de roller vid ITS eller andra enheter och institutioner som krävs i incidenthanteringen, exempelvis systemägare, förvaltningsledare, drift och systemadministrativ personal mm.

IRT ska löpande informera IT-chef och övriga nyckelpersoner - som utsetts av IT-chef - om pågående kritiska cybersäkerhetsincidenter. IT-chef ansvarar för att informationen eskaleras till mottagare i universitetsledningen, om det finns behov att informera om eller samordna hanteringen.

Dataskyddsombud vid Enheten för juridik och informationsförvaltning (JIF)

Dataskyddsombudet vid Enheten för juridik och informationsförvaltning ger råd och stöd vid analys och hantering av personuppgiftsincidenter och ansvarar för anmälan av personuppgifts incidenter till Integritetskyddsmyndigheten (IMY).

Säkerhetsfunktionen vid Lokalförsörjningsenheten (LOK)

Säkerhetsfunktionen vid Lokalförsörjningsenheten ger råd och stöd vid analys och hantering av fysiska säkerhetsincidenter och säkerhetsskyddsincidenter.

Säkerhetsfunktionen ansvarar för att eskalera till mottagare i universitetsledningen om det finns behov att informera universitetsledning eller samordna hanteringen.

HR-stöd vid Personalenheten

HR-stöd vid Personalenheten ger råd och stöd vid sådana fysiska säkerhetsincidenter som kan innebära skada för personal.

3.2 Roller och funktioner vid eskalerad incidenthantering

IT-chef och krisgrupp för IT

Vid större cyberssäkerhetsincidenter utser IT-chef eller av denna utpekade nyckelpersoner en incidentledare som leder och samordnar hanteringen tillsammans med IRT samt aktiverar vid behov krisgrupp för IT (ITS krisgrupp).

Incidentledaren eller krisgruppen analyserar verksamhetspåverkan och konsekvenser samt informerar och involverar vid behov andra berörda verksamheter och roller exempelvis systemägare vid berörd institution, dataskyddsombud mfl.

Incidentledaren beslutar om kontakt ska tas med CERT-SE, Sveriges nationella CSIRT, eller annan extern aktör, för stöd i incidenthanteringen.

IT-chef eller incidentledaren informerar mottagare i universitetsledningen om krisgrupp har aktiverats för hantering av cyberssäkerhetsincident.

Mottagare i universitetsledningen och universitets krisledningsgrupp

Incidenter som involverar flera säkerhetsområden eskaleras vid behov till mottagare i universitetsledningen som samordnar incidenthanteringen mellan de olika säkerhetsområdena.

Mottagare i universitetsledningen beslutar om incidenthantering ska övergå till krishantering enligt universitetets regel för krishantering. De ytterligare roller som behövs i krisledningens hantering av säkerhetsincidenten adjungeras.

3.3 Övriga roller och funktioner som involveras vid behov

Kommunikationsenheten

Bistår vid behov med att informera interna och externa intressenter.

Informationssäkerhetssamordnare vid Enheten för juridik och informationsförvaltning (JIF)

Informationssäkerhetssamordnaren kan vid behov stödja vid analys av informationssäkerhetsincidenter. Informationssäkerhetssamordnaren ska sammanställa statistik över cybersäkerhetsincidenter och ska efter allvarliga eller betydande cyberssäkerhetsincidenter ta del av den dokumenterade utvärderingen som underlag för uppföljning och gemensamt förbättringsarbete inom ramen för ledningssystemet för informationssäkerhet (LIS).

4. Vidarerapportering av säkerhetsincidenter

Universitet har skyldighet att göra anmälan till olika myndigheter när vissa typer av säkerhetsincidenter har inträffat. Denna inrapportering samordnas i de flesta fall centralt och beskrivs nedan.

4.1 Anmälan av IT- eller cybersäkerhetsincidenter

IT- eller cyberssäkerhetsincidenter enligt Checklista identifiering av rapporteringspliktig it- eller cybersäkerhetsincident ska rapporteras till Nationellt cybersäkerhetscenter (NCSC) vid Försvarets radioanstalt (FRA). Inledningsvis genom en upplysning inom 6 respektive 24 timmar från att incidenten identifierats som anmälningspliktig.

IRT bedömer initialt om en incident är anmälningspliktig och lämnar den initiala upplysningen till NCSC. IRT gör även tillsammans med eventuell incidentledare vid ITS en kompletterande incidentanmälan (inom 72 timmar) samt bereder slut- eller lägesrapport (inom 1 månad) enligt gällande regler.

4.1.1 Informationsskyldighet

Om en betydande cyberssäkerhetsincident har påverkat en eller flera externa tjänster som universitet tillhandhåller till mottagare alternativt ett betydande cyberhot kan påverka system som universitetet tillhandahåller till mottagare, ska mottagarna så snart som möjligt informeras, så länge informationen inte kan försvåra hanteringen eller förvärra dess konsekvenser.

Information om vad incidenten eller hotet består i, vilka åtgärder som mottagarna behöver vidta och konsekvenser om de inte vidtas ska lämnas.

Aktiverad krisgrupp bedömer tillsammans med IRT om och hur informationen kan ges.

4.2 Anmälan av personuppgiftsincidenter

En personuppgiftsincident ska anmälas till Integritetsskyddsmyndigheten (IMY) inom 72 timmar från vetskap om incidenten, såvida det inte är osannolikt att den medfört en risk för fysiska personers rättigheter och friheter.

Dataskyddsombudet bedömer om en incident är anmälningspliktig och anmäler personuppgiftsincidenter till Integritetsskyddsmyndigheten IMY enligt gällande regler.

Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige som utgångspunkt utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten i enlighet med Dataskyddsförordningen artikel 34.

När UMU är personuppgiftsbiträde ska UMU rapportera till personuppgiftsansvarig i enlighet med villkoren personuppgiftsbiträdesavtalet.

4.2.1 Rapportering vid utkontraktering

Om universitetet överlåter en del av sin informationshantering till en aktör som inte omfattas av anmälningsskyldighet enligt ovan ska universitetet säkerställa att aktören åtar sig att rapportera säkerhetsincidenter till universitetet på ett sådant sätt att universitetet kan uppfylla kraven på rapportering.

4.3 Anmälan vid incidenter rörande säkerhetsskydd

Anmälningspliktiga säkerhetsskyddsincidenter ska skyndsamt anmälas till Säkerhetspolisen. Säkerhetsfunktionen vid Lokalförsörjningsenheten bedömer om en incident är anmälningspliktig och anmäler till Säkerhetspolisen enligt gällande regler.

4.4 Anmälan vid svårare personskador mm

Om en säkerhetsincident inneburit att en allvarlig personskada, skador som har drabbat flera medarbetare samtidigt samt allvarliga tillbud eller dödsfall inträffat ska berörd chef alltid anmäla detta utan dröjsmål till Arbetsmiljöverket enligt instruktion ’Hantera arbetsskada, tillbud och riskobservation’ på medarbetarwebben.

Bilaga 1 – Definition av säkerhetsincidenter

En säkerhetsincident är en oönskad och oplanerad händelse som påverkar, eller kan komma att påverka, säkerheten negativt för universitetets skyddsvärda tillgångar dvs medarbetare, studenter, information, informationssystem, lokaler och utrustning. En säkerhetsincident kan även innebära en störning i universitetets förmåga att bedriva sin verksamhet.

Det finns flera typer av säkerhetsincidenter vilka beskrivs nedan. En inträffad incident kan påverka flera säkerhetsområden och vara av flera incidenttyper samtidigt.

1. Fysisk säkerhetsincident

En fysisk säkerhetsincident utgörs ofta av händelser som är till skada för person eller egendom. Exempel på fysiska säkerhetsincidenter kan vara hat, hot, våld, olaga intrång, inbrott, stöld, skadegörelse, sabotage, brand samt intrång i säkerhetskänslig verksamhet.

2 Säkerhetsskyddsincident

En säkerhetsskyddsincident är en händelse som innebär att säkerhetskänslig verksamhet eller säkerhetsskyddsklassificerad information har utsatts för obehörig åtkomst, skada eller risk för att röjas. Säkerhetskänslig verksamhet eller säkerhetsklassificerad information är sådan som har betydelse för Sveriges säkerhet.

3. Informationssäkerhetsincident

En informationssäkerhetsincident är en oönskad händelse med negativa konsekvenser som inträffar när skyddet av information inte är tillräckligt. Det kan påverka konfidentialiteten, riktigheten eller tillgängligheten för informationen, dvs innebära att obehöriga fått åtkomst till information,
att information är felaktig, eller att den inte går attkomma åt. Det gäller alla typer av infor mation, inte bara information i IT-system.

4. IT-säkerhetsincident

En IT-säkerhetsincident är en händelse som påverkar säkerheten i ett IT-system, till exempel intrång, skadlig kod (malware), överbelastnings-attacker eller obehörig åtkomst till system och data.

5. Personuppgiftsincident

En personuppgiftsincident är en säkerhetsincident som rör personuppgifter. Det kan innebära att personuppgifter har blivit förstörda eller ändrade, gått förlorade eller kommit i orätta händer.

En personuppgiftsincident kan till exempel vara en hackerattack där uppgifter från ett system blir stulna, en borttappad mobiltelefon, att personal som inte har behörighet att se

personuppgifter av misstag får tillgång till sådana uppgifter eller att ett mail innehållande personuppgifter skickas till fel person.

6. Cybersäkerhetsincident

En cybersäkerhetsincident är en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter i nätverks- och informationssystem. En cyberssäkerhetsincident är m a o både en informationssäkerhetsincident och en IT-säkerhetsincident samt kan även innebära att en personuppgiftsincident och en fysisk eller säkerhetsskyddsincident samtidigt har inträffat.

6.1 Betydande cybersäkerhetsincident

En cybersäkerhetsincident är betydande om den har orsakat eller kan orsaka allvarlig driftstörning, ekonomisk skada för universitetet eller om den påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada.