Dokumenttyp: Rutin	Beslutsdatum: 2023-11-15
Beslutsfattare: Säkerhetschef	Träder i kraft: 2023-11-15
Avdelning/kansli: Avdelningen för infrastruktur	Giltighetstid: Tills vidare
Handläggare: Marcus Nilsson	Bör uppdateras före: 2026-11-15

Rutin för rapportering av it-incidenter

1. Inledning

Denna rutin syftar till att beskriva tillvägagångssätt och handläggningsordningen för rapporteringen av it-incidenter vid SLU. Rutinen riktar sig dels till incidentanmälare av it-incidenter, dels till incidentsamordnare som hanterar it-incidenter.

Rutinen redogör för vilka kommunikationsvägar och stödsystem som ska användas vid rapporteringen av it-incidenter (för incidentanmälare). Rutinen beskriver även arbetsflödet vid extern it-incidentrapportering, eskalerings- och återkopplingsprocesser, samt vägledande principer för dokumentation och kommunikation (för incidentsamordnare).

Rutinen kompletterar SLU:s riktlinjer för rapportering av it-incidenter och IT-avdelningens it-incidenthanteringsprocess.[1]

2. Terminologi

Term	Definition
Allvarlig it-incident	En it-incident som omfattas av rapporteringsskyldighet enligt bestämmelserna i MSBFS 2020:8. En allvarlig it-incident ska rapporteras till Myndigheten för samhällsskydd och beredskap (MSB) och avser en it-incident som 1. påverkat riktigheten, tillgängligheten eller konfidentialiteten hos den

[1] Se SLU.ua.2022.1.1.1-3502 Riktlinjer för rapportering av it-incidenter, dokumentet ”Incident Management” (saknar diarienummer), samt SÄK AL M 002 Manual för MSB-ärende.

	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. En ”major incident” enligt ramverket ITIL kan föranleda, eller sammanfalla med, en allvarlig it-incident.[2]
Incidentanmälare	Den person som upptäcker en it-incident och som ska anmäla incidenten.
Incidentsamordnare	Den person som har ett sammanhållande ansvar för det övergripande och operativa arbetet med it-incidenten. Jämför rollen ”Incident Manager”.[3]
Informationssäkerhetsincident	En enskild eller flera oönskade eller oväntade informationssäkerhetshändelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet (SS-EN ISO/IEC 27000:2020).
It-incident	En oönskad och oplanerad it-relaterad händelse som kan påverka säkerheten i SLU:s informationshantering och som kan innebära en störning i SLU:s förmåga att bedriva sin verksamhet. Exempel är störningar i driftsmiljöer, mjuk- eller hårdvara, informationsläckage, säkerhetsbrister i produkter, eller angrepp med skadlig kod. En it-incident kan föranleda, eller sammanfalla med, en informationssäkerhetsincident eller en personuppgiftsincident. Jämför även allvarlig it-incident.

[2] Jämför definitionen av ”major incident” i dokumentet ”Incident Management”.
[3] Se vidare dokumentet ”Incident Management”.

Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats (artikel 4 dataskyddsförordningen).

3. Avgränsning

Denna rutin omfattar inte rapportering av it-incidenter i informationssystem som har betydelse för säkerhetskänslig verksamhet enligt 2 kap. 4 § första stycket 2 säkerhetsskyddsförordningen (2021:955). Rapportering av sådana incidenter sker i särskild handläggningsordning till SLU Säkerhet enligt instruktion för säkerhetsskydd.[4]

4. Att rapportera it-incidenter (för incidentanmälare)

Alla anställda, studenter eller medarbetare som arbetar på uppdrag av SLU har ansvar för att skyndsamt rapportera upptäckt av it-incident.

Rapportering utförs enligt följande processteg:

1. Rapportera it-incidenten till e-postadressen support@slu.se. En incidentanmälan bör innehålla en övergripande beskrivning av incidenten och, i tillämpliga fall, vilken information som har påverkats.

    1.1. I händelse av driftstörning i SLU:s e-posttjänst eller motsvarande, rapportera it-incidenten till it-supporten via telefonnummer 018-67 6600 tonval 1.

2. Om it-incidenten har påverkat personuppgifter, gör en kompletterande incidentrapport om en personuppgiftsincident i IA-systemet. Rapporteringen bör göras så snart som möjligt.

    2.1. I händelse av driftstörning i IA-systemet eller motsvarande, rapportera personuppgiftsincidenten till e-postadressen dataskydd@slu.se eller telefonledes till dataskyddsjurist.

[4] SLU.ua.2019.2.10-2896 Instruktion för säkerhetsskydd.

4.1. Rapportering av övriga avvikelser av betydelse för informationssäkerheten

Om du upptäcker avvikelser av teknisk eller administrativ karaktär, som kan påverka säkerheten i SLU:s informationshantering, rapporteras avvikelsen i IA-systemet.

Exempel på avvikelser är bristfälliga rutiner för hantering av skyddsvärd information, olämplig exponering av information för obehöriga, eller brister i fysiska säkerhetsåtgärder som är avsedda att skydda information.

En rapporterad avvikelse kan, efter bedömning av SLU Säkerhet, övergå i en informationssäkerhetsincident.

5. Att hantera rapporterade it-incidenter (för incidentsamordnare)

Rutin för handläggning av it-incidenter vid SLU framgår av IT-avdelningens it-incidenthanteringsprocess.[5] I it-incidenthanteringsprocessen redovisas bl.a. SLU:s system för prioritering av it-incidenter utifrån kriterier för brådska och påverkan. Processen beskriver även IT-avdelningens interna roll- och ansvarsfördelningar vid it-incidenthantering.[6]

Prioriterings- och kategoriseringsmodell för allvarliga it-incidenter som omfattas av rapporteringsskyldighet till MSB finns i rutinbeskrivningen för kategorisering av MSB-ärenden.[7] Roller, ansvar och övergripande arbetssätt för hanteringen av sådana it-incidenter beskrivs i SLU:s riktlinjer för rapportering av it-incidenter.[8]

I föreliggande avsnitt beskrivs rutiner för rapportering och hantering av it-incidenter som kompletterar de befintliga styrningarna i ovan angivna styrdokument. Målgruppen för rutinerna är incidentsamordnare.

5.1. Rapportering av allvarliga it-incidenter till MSB

I enlighet med SLU:s riktlinjer för rapportering av it-incidenter ansvarar IT-avdelningen för rapportering till MSB. SLU Säkerhet stödjer i incidentbedömningen och i framtagningen av slutrapporten till MSB.

Rapporteringen utförs enligt följande processteg:

1. Notifiera MSB via verktyget IRON inom sex timmar från det att incidenten upptäcks.

    1.1. I händelse av driftstörning i IRON eller motsvarande, notifiera MSB (CERT-SE) om incidenten via telefonnummer 010-240 40 40.

[5] Se dokumentet ”Incident Management”.
[6] Se s. 16ff och s. 22f i ”Incident Management”.
[7] SÄK AL M 002 Manual för MSB-ärende.
[8] SLU.ua.2022.1.1.1-3502 Riktlinjer för rapportering av it-incidenter.

2. Slutrapportera incidenten till MSB via verktyget IRON inom fyra veckor.

    2.1. I händelse av driftstörning i IRON eller motsvarande, skicka slutrapporten via rekommenderat brev till adressen:

    Myndigheten för samhällsskydd och beredskap
    CERT-SE
    Box 6081
    171 06 Solna

5.2. Återkoppling till incidentanmälare

I syfte att bygga en god rapporteringskultur vid SLU ska varje incidentanmälare av it-incidenter motta en lämplig och lättbegriplig återkoppling om den rapporterade incidenten. Incidentanmälaren ska löpande och i relevant omfattning underrättas om statusen på incidenten. Incidentsamordnaren för incidenten ansvarar för återkoppling till incidentanmälaren.

5.3. Kommunikation med externa och interna parter om inträffade it-incidenter

Som huvudregel gäller att informationsdelning med externa parter om inträffade it-incidenter vid SLU ska ske restriktivt. Särskild hänsyn ska tas till gällande sekretessbestämmelser om upplysningar om säkerhets- och bevakningsåtgärder i informationssystem.[9] Incidentsamordnare för it-incidenter ansvarar för att genomföra sekretessbedömningar för uppgifter rörande it-incidenter. Samråd om sekretessbedömningar kan vid behov sökas med juristenheten.

Om den inträffade incidenten är av en sådan karaktär att informationsspridning om den bedöms kunna främja andra organisationers cyberresiliens, får uppgifter om incidenten kommuniceras externt efter sekretess- och lämplighetsbedömning. Samråd om bedömningen ska sökas med SLU Säkerhet och juristenheten.

Vid intern kommunikation inom SLU om inträffade it-incidenter gäller principen om behovsbaserad åtkomst.

5.4. Dokumentation av it-incidenter

It-incidenter ska dokumenteras i den utsträckning det behövs för att mäta och övervaka återkommande typer av incidenter, dess orsaker, kostnader och omfattning. I dokumentationen bör även ingå lärdomar som kan dras av incidenten.

[9] Se 18 kap. 8 § offentlighets- och sekretesslagen (2009:400).

Dokumentationens syfte är att möjliggöra samlade utvärderingar av inträffade it-incidenter, identifiera generella informationssäkerhetsrisker, samt bidra till förbättringar av rutiner, arbetssätt och säkerhetsåtgärder.

Dokumentation om it-incidenter ska tillgängliggöras till ansvarig för ledningen och samordningen av informationssäkerhetsarbetet (SLU Säkerhet).[10]

5.5. Hantering av bevis i samband med it-incidenter

I fall där disciplinära eller rättsliga åtgärder kan behöva vidtas som en följd av en it-incident ska information som kan utgöra bevismaterial hanteras aktsamt. Detta i syfte att säkerställa informationens fullständighet och riktighet. I samband med hanteringen av en it-incident behöver därför en restriktiv hållning intas kring t.ex. radering och förlustgivande konvertering av information med ett möjligt bevisvärde.

5.6. Eskalering till kris

Med kris avses en oförutsedd händelse som det inte finns handlingsberedskap för, som inte kan hanteras med invanda rutiner och som riskerar att orsaka stor skada på människa, miljö, ekonomi eller på förtroendet för SLU.[11] I de fall en allvarlig it-incident bedöms utgöra en kris ska SLU:s krisorganisation aktiveras. I händelse av kris ansvarar säkerhetschefen för beslut om akuta åtgärder, i samråd med berörd krisgrupp.

[10] Jfr MSB:s allmänna råd i MSBFS 2020:6.
[11] SLU.ua.2015.1.1.1-2460 Riktlinjer för krishantering och krisorganisation vid SLU.