Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

STYRANDE DOKUMENT SLU ID: SLU.ua.2022.1.1.1-3502

Sakområde: Säkerhet och informationssäkerhet

Dokumenttyp: Riktlinjer	Beslutsdatum: 2022-10-14
Beslutsfattare: Universitetsdirektören	Träder i kraft: 2022-10-14
Avdelning/kansli: SLU Säkerhet	Giltighetstid: Tills vidare
Handläggare: Informationssäkerhetsstrateg Marcus Nilsson	Bör uppdateras före: 2025-10-14

Ev dokument som upphävs: SLU.ua.2016.2.10-1231 Riktlinje för rapportering av säkerhetspåverkande IT-incident

Bilaga till: Beslut om Riktlinjer för rapportering av it-incidenter

Riktlinjer för rapportering av it-incidenter

1. Inledning

Föreliggande riktlinjer anger tillvägagångssätt och ansvarsförhållanden vid rapportering av it-incidenter vid SLU. Riktlinjerna vänder sig till samtliga SLU:s medarbetare, studenter och övriga inom SLU:s verksamheter.

Med it-incident avses 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.

Med allvarlig it-incident avses i det följande en incident som omfattas av rapporteringsskyldighet enligt bestämmelserna i MSBFS 2020:8. Allvarliga it-incidenter ska rapporteras till Myndigheten för samhällsskydd och beredskap (MSB).

En it-incident kan föranleda, eller sammanfalla med, en informationssäkerhetsincident eller en personuppgiftsincident.[1] Sådana

[1] Med informationssäkerhetsincident avses en enskild eller flera oönskade eller oväntade informationssäkerhetshändelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet (SS-EN ISO/IEC 27000:2017). En personuppgiftsincident är 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).

incidentärenden aktualiseras vid förlust av konfidentialitet, riktighet eller tillgänglighet för skyddsvärd information, till exempel känsliga personuppgifter.

2. Avgränsning

Dessa riktlinjer 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.

3. Ansvar

Verksam vid SLU

Alla anställda, studenter eller medarbetare som arbetar på uppdrag av SLU har ansvar för att skyndsamt rapportera upptäckt av it-incident. Rapportering ska ske enligt instruktion för rapportering av it-incidenter.

It-avdelningen

It-avdelningen ansvarar för upprätthållande av it-säkerhetsfunktionen som tar emot, bedömer, åtgärdar och utreder orsakerna till rapporterade incidenter. De hanterar SLU:s vidare rapportering till MSB och är mottagare av återkoppling, varningar och begäran om komplettering från MSB.

SLU Säkerhet

SLU Säkerhet kravställer rapportering internt inom SLU för att säkerställa att SLU efterlever MSB:s föreskrifter om rapportering av it-incidenter för statliga myndigheter (MSBFS 2020:8).

Dataskyddsfunktionen

Dataskyddsfunktionen vid SLU stödjer vid incidenter i informationssystem som innehåller personuppgiftsbehandlingar. Dataskyddsfunktionen deltar i hela processen för att hantera en personuppgiftsincident och ansvarar även för eventuell anmälan till Integritetsskyddsmyndigheten (IMY).

4. Övergripande tillvägagångssätt vid rapportering

När en it-incident upptäcks är det varje persons ansvar att skyndsamt rapportera till it-säkerhetsfunktionen enligt instruktion för rapportering av it-incidenter.

Vid it-säkerhetsfunktionen sker samordning, analys och enhetlig bedömning av incidenten. I de fall incidenten bedöms som allvarlig lämnar it-säkerhetsfunktionen en notifiering till MSB inom sex timmar. I samråd med SLU Säkerhet ansvarar it-säkerhetsfunktionen för att slutrapportera incidenten till MSB inom fyra veckor.

MSB kan således få en samlad och övergripande bild över händelser och samordnat vidta åtgärder för att avvärja eller begränsa konsekvenser av allvarliga it-incidenter i samhället.

Vid hantering av it-incidenter som har påverkat sekretessen, integriteten eller tillgängligheten till personuppgifter ska it-säkerhetsfunktionen rådgöra med dataskyddsfunktionen. Dataskyddsfunktionen ansvarar för bedömning av personuppgiftsincidentens skadeverkan och, i förekommande fall, anmälan till IMY. En personuppgiftsincident ska anmälas till IMY inom 72 timmar från det att den blev känd. Kompletterande uppgifter rörande en anmäld personuppgiftsincident kan vid behov lämnas till IMY inom fyra veckor.

5. Rapportering vid utkontraktering

När en extern aktör hanterar SLU:s information ska aktören rapportera allvarliga it-incidenter till SLU i enlighet med MSBFS 2020:8. Skyldigheten att rapportera sådana incidenter ska regleras i avtal med aktören.

Om en aktör behandlar personuppgifter i informationssystem för SLU:s räkning i egenskap av personuppgiftsbiträde ska krav på rapportering av personuppgiftsincidenter till SLU regleras i personuppgiftsbiträdesavtal.