Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

GOVERNING DOCUMENT SLU ID: SLU.ua.2022.1.1.1-3502

Subject area: Security and information security

Document type: Guidelines	Decision date: 14/10/2022
Decision-maker: Chief Operating Officer	Effective as of: 14/10/2022
Organisational unit: SLU Security	Valid until: Further notice
Reference: Information Security Strategist Marcus Nilsson	To be updated by: 14/10/2025

Document(s) repealed: SLU.ua.2016.2.10-1231 Riktlinje för rapportering av säkerhetspåverkande IT-incident

Annex to: Beslut om Riktlinjer för rapportering av it-incidenter

Guidelines for reporting IT incidents

1. Introduction

These guidelines establish the procedures and division of responsibilities for reporting IT incidents at SLU. They are aimed at all staff members, students and others active at SLU.

The term “IT incident” refers to an unwanted and unplanned IT-related event that could affect the security of SLU's information management and cause disruption in SLU's ability to conduct its operations. Some examples include disruptions to operational environments, software or hardware, information leakages, security defects in products, or malware attacks.

The term “serious IT incident” refers in the following to an incident that is covered by a reporting obligation in accordance with the regulations in MSBFS 2020:8. Serious IT incidents must be reported to the Swedish Civil Contingencies Agency (MSB).

An IT incident may lead to, or coincide with, an information security incident or a personal data breach.[1] Such incidents and breaches occur where there is a loss of confidentiality, integrity or availability of information worthy of protection, for example sensitive personal data.

[1] An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security (SS-EN ISO/IEC 27000:2017). A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (Article 4 GDPR).

2. Delimitations

These guidelines does not apply to IT incident reporting in information systems relevant to security-sensitive activities in accordance with Chapter 2, Section 4, first paragraph, point 2, of the Protective Security Ordinance (2021:955). These incidents must be reported to SLU Security as per the administrative procedures outlined in the instructions for protective security.

3. Responsibility

Everyone at SLU

All employees, students or staff members working on behalf of SLU are responsible for reporting any IT incidents immediately following their detection. Reporting must follow the instructions for IT incident reporting.

Division of IT

The Division of IT is responsible for maintaining the IT security function which receives, assesses, acts upon and investigates the causes of reported incidents. The division is responsible for reporting incidents to MSB and is the point of contact for feedback and warnings. The division will also provide MSB with additional information upon request.

SLU Security

SLU Security establishes requirements for reporting internally at SLU in order to ensure that SLU complies with MSB's regulations on IT incident reporting for government agencies (MSBFS 2020:8).

Privacy and data protection function

The privacy and data protection function at SLU provides support in the event of incidents involving processing of personal data in information systems. The privacy and data protection function participates in the whole process of managing a personal data breach and is furthermore responsible for making notifications to the Swedish Authority for Privacy Protection (IMY).

4. General reporting procedure

When an IT incident is detected, everyone at SLU is obliged to immediately report to the IT security function as per the instructions for IT incident reporting.

The IT security function will coordinate, analyse and continually assess the incident. If the incident is considered serious, the IT security function will notify MSB within six hours. The IT security function is responsible for submitting a final incident report to MSB within four weeks, following consultation with SLU Security. This enables MSB to determine a collected and comprehensive overview of incident occurrences and coordinate actions to avert and limit the consequences of serious IT incidents in society.

When managing IT incidents which have affected the secrecy, integrity or availability of personal data, the IT security function must consult the privacy and data protection function. The privacy and data protection function is responsible for assessing the impact of the personal data breach and, where appropriate, notifying IMY. A personal data breach must be notified to IMY within 72 hours after SLU has become aware of it. Supplementary information regarding a previously made data breach notification can be submitted to IMY within four weeks.

5. Reporting procedures in outsourcing arrangements

When an external party processes SLU's information, the party must report serious IT incidents to SLU in accordance with the terms in MSBFS 2020:8. The obligation to report such incidents is to be regulated in an agreement with the external party.

If a party processes personal data in information systems on behalf of SLU, thus acting as a data processor, requirements for breach notifications to SLU must be defined in the data processing agreement.