This document is a translation. The official version is in Swedish.

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

GOVERNING DOCUMENT SLU ID: SLU.ua.2023.2.10-2023

Subject area: 11. IT/Service/Security/Environment

Document type: Policy	Decision date: 14/06/2023
Decision-maker: Vice-Chancellor	Effective as of: 14/06/2023
Organisational unit: Division of Infrastructure	Valid until: Further notice
Reference: Marcus Nilsson	To be updated by: 14/06/2026

Document(s) repealed: SLU ua 2015.2.10-2118 Riktlinjer för informationssäkerhet vid SLU

Annex to: Vice-chancellor's decision on information security policy for the Swedish University of Agricultural Sciences

Information security policy for the Swedish University of Agricultural Sciences

1. Introduction

In this information security policy, the vice-chancellor sets out the intentions of information security efforts at the Swedish University of Agricultural Sciences (SLU).

SLU's vision is to play a key role in the development for sustainable life, based on science and education. Our information security work will support this vision by proportionally balancing academic openness and the need to protect the university's information. Information security is defined as protecting information from unauthorised access or change, and ensuring it is available to those who need it when they need it.

All information security work done at the university must be risk-based, and SLU is to have an information security management system based on the standards ISO/IEC 27001 and ISO/IEC 27002. Where applicable, other related standards on information and IT security should also be used.

The university's information is to be protected as follows:

Confidentiality – avoiding information being disclosed or made available to unauthorised individuals.

Integrity – ensuring information is not changed, be it due to mistake, functional error or unauthorised access.

Availability – ensuring information is available to authorised users when they need it.

Through this policy, the university commits to continually improving the information security management system and fulfilling applicable information security requirements. To support the implementation of security measures under the management system, the policy is supplemented with plans, rules, procedures or other internal governing documents of importance to information security work at the university.

2. Target group

The target group comprises all staff, students and other individuals who manage information at the university.

3. Objectives

These are SLU's strategic information security objectives:

- Our information is identified and classified as per the university's information classification model.
- Information security risks that affect the university are known, assessed and treated as defined in our risk management model.
- Our information and information systems are suitably protected.
- Our research, teaching and support operations take information security into account.
- We have a mature information security culture.

The strategic information security objectives are converted to implementable, short-term annual objectives.

4. Roles and responsibilities

The **vice-chancellor** has the main responsibility for information security at SLU but will delegate responsibility and decision-making powers as per the vice-chancellor's delegation of authority. The vice-chancellor is responsible for keeping themselves informed about the status of information security activities under the applicable regulations.

The **chief operating officer** appoints a member of staff to lead and coordinate information security work. The chief operating officer is responsible for ensuring that this person has the necessary decision-making power and resources at their disposal.

The **head of security** and the **head of protective security** are responsible for decisions on emergency measures. The head of security is responsible for information security in areas related to the university's protective security work.

The **IT director** decides on rules for IT security. The IT director reports on the status of the university's IT security to the person(s) appointed to lead and coordinate the information security work.

Operational managers are responsible for information security within their operations. This means managing information security based on their knowledge of operations as well as the protection value of information. Operational managers include heads of department and equivalent.

Information owners are responsible for classifying information, assessing risks and appropriately protecting information. Information owners are operational managers, or someone appointed by them, with responsibility for the operational process where information is created and managed. The information owner is also the risk owner to the extent the risk can be attributed to their operations. For university-wide information security risks, the vice-chancellor appoints a risk owner.

The **system owner** is responsible for overall information security in their respective information system. They are consequently responsible for compliance with applicable requirements for the information system concerned, based on an information classification and a risk assessment. The system owners are the operational managers, or someone appointed by them, with responsibility for the operational process that is supported by the information system.

All SLU staff and students are responsible for protecting information in accordance with this policy and for contributing to a sound information security culture.

5. Non-conformities and exceptions

The information security policy describes the university's basic information security requirements. Only the vice-chancellor can decide on derogations and exceptions from this policy. Such decisions must be documented in writing.

6. Monitoring and compliance

The information security policy will be reviewed every three years or when risk factors, regulations or other conditions that affect the university's information security change. Compliance with the policy will be checked at regular intervals.