Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

GOVERNING DOCUMENT

SLU ID: SLU.ua.2025.1.1-315

Version no.: 1.0.2

Subject area: IT/Service/Security/Environment

Document type: Rule
Decision-maker: Chief Operating Officer
Organisational unit: Division of IT
Decision date: 28 January 2025

Effective as of: 3 February 2025
Valid until: Further notice
Last reviewed: 28 January 2025
To be reviewed by: 28 February 2026

Document(s) repealed: –

Annex to: Chief Operating Officer's decsion, 28 January 2025, SLU.ua.2025.1.1-315

Rules for the acceptable use of IT resources

Target group and purpose

All users of the university's IT resources (employees, students, contractors, partners and other users) must adhere to these rules defining acceptable use.

The rules intend to ensure the secure and acceptable use of SLU's IT environment, and protect the university's information, assets and intellectual property. At the same time, the rules will enable all users to work efficiently and securely. In many cases, boundaries may be blurred, meaning the user's own judgement is important.

Summary

The document clarifies that the following constitute unauthorised use:

- illegal activities
- malware and attacks
- unauthorised access and hacking
- overloading traffic and network abuse
- harassment and malicious communication
- prohibited information sharing and storing
- prohibited software use.

Some automated monitoring is conducted to ensure compliance and enable follow-up and management of incidents. All use must be in accordance with applicable

legislation and other university regulations. Disciplinary measures may be taken in the event of the rules being broken.

Scope

These rules clarify and establish what constitutes authorised use of the university's IT resources. IT resources include, but are not limited to, physical hardware (computers, servers, networks, mobile phones, etc.), services and apps. These rules apply to SLU's IT resources regardless of where the user is located.

All users of SLU's IT resources undertake to comply with these rules. The rules are part of SLU's information security management system.

Acceptable use

SLU's services and systems may only be used for legitimate and authorised purposes that are consistent with the university's objectives. Their use must comply with the applicable law. Acceptable use includes the following:

- Performing work tasks or duties related to SLU's activities.
- Using SLU email accounts for communication for work purposes. Private use of an SLU email account may be permitted to a certain extent.
- Using SLU's network and resources within the framework of SLU's activities. Other use must be within reason.

Unauthorised use

Illegal activities

Using SLU's services, systems or networks to conduct or facilitate illegal activities is prohibited. Such activities include:

- fraud, identity theft or unauthorised attempts to obtain information;
- distribution or providing access to illegal materials such as pirated software, films, music or other copyrighted works.

Malware and attacks

It is prohibited to use SLU's equipment, systems and services to initiate or distribute malicious code (malware), viruses, trojans, ransomware or other software intended to damage, disrupt or gain unauthorised access to networks or systems. Misusing SLU's IT resources is also forbidden for committing illegal data access at SLU or other party.

Unauthorised access and hacking

All attempts to gain unauthorised access to systems, networks or data are strictly prohibited. These include:

- attempts to circumvent security measures or restrictions implemented to protect the network;
- attempts to breach systems or servers, both within and outside the university network;
- phishing or other fraudulent measures to gain unauthorised access to sensitive information.

Denial of service and network abuse

It is prohibited to use university resources to overload, disrupt or negatively affect network capacity, performance or stability. This includes:

- participating in or creating denial of service attacks (DDoS);
- intentionally or unintentionally creating excessive network traffic that affects the quality of services.

Harassment and malicious communication

SLU's services must never be used to spread offensive, threatening, harassing or insulting messages such as:

- junk email, mass emails or unsolicited marketing (spam);
- stalking, bullying or threatening other users or third parties using SLU's services.

Prohibited information sharing and storing

The following is prohibited:

- Sharing classified as secret, copyrighted or otherwise confidential information with an unauthorised person.
- Sharing personal data, especially sensitive personal data of which SLU is the processor, with internal or external recipients who are not authorised and do not need access to the personal data.

Prohibited software use

IT resources connected to the university's network (computers, mobile phones, tablets, etc.) should be updated with the latest operating system and software. The minimum requirement is for the version to be supported, thus having the latest security update. If this is not possible, exceptions must be reported via support.slu.se and adequate security measures taken.

SLU reserves the right to uninstall software or wipe devices that do not comply with the rules.

The following is prohibited:

– Change the configuration, remove, disable, or otherwise manipulate security protections or other software.
– Downloading and using software that is not properly licensed.

Responsibilities

All users have a responsibility to protect the university's systems and data by:

- not sharing their login details with unauthorised individuals;
- reporting any issues or incidents on support.slu.se or support@slu.se;
- protecting their devices from viruses and malware;
- ensuring that communication and data transfer are secure and encrypted when possible.

Secrecy and confidentiality

Disclosing classified information as defined in the Public Access to Information and Secrecy Act is a breach of duty of confidentiality. The duty of confidentiality means a person must not disclose or use classified information, neither orally nor otherwise. Breaches of the statutory duty of confidentiality are penalised in accordance with The Swedish Criminal Code.

Monitoring and reporting

SLU reserves the right to monitor the use of the university's IT resources to ensure compliance with these regulations. Examples include:

- monitoring network traffic, logs and other relevant information;
- monitoring email, files and other communication relating to the university's activities.

Monitoring complies with the applicable legislation and is automatic, without human intervention except in the event of abnormalities and incidents.

Disciplinary measures

Violations of these rules may result in disciplinary measures being taken. These include temporary suspension of an SLU user account, disconnection of computer equipment, telephone or similar IT resource.

Serious infringements constituting criminal offences, disclosure of information classified as secret, will be addressed by the staff or student disciplinary board.

Changes to the regulations

This document will be updated as necessary. Users will be notified of any significant changes and the latest version will be available on the staff web and/or other communication channels.

Contact information

For questions about document and IT security contact csirt@slu.se.

For questions about information security sakerhet@slu.se.
For questions on data protection and the general Data Protection Regulation (GDPR), contact dataskydd@slu.se.

Contact support@slu.se for support and in the event of anomalies or incidents. Alternatively, visit support.slu.se.