



JÖNKÖPING UNIVERSITY

Declaration of Responsibility for the Use of the University's Computer, Network, and System Resources

Student – 2026-06-04

Purpose and Background

This declaration of responsibility governs the use of the IT resources of Jönköping University (hereinafter referred to as the University), identities within the SWAMID federation, and connections to SUNET.

The purpose of assigned computers, user accounts, email, and other IT resources is to support the conduct of studies, teaching, and related academic activities. The IT resources constitute part of the organization's shared infrastructure and shall be used in a responsible, secure, and appropriate manner. Use shall, in particular, ensure:

- secure and correct use of IT resources
- protection of the organization's and third parties' information
- compliance with the SWAMID trust framework
- compliance with SUNET's ethical rules for the use of networks and resources

Use shall furthermore take place in accordance with applicable legislation and internal governing documents and contribute to maintaining the availability, integrity, and trust in the organization's IT environment and connected services.

The IT resources may not be used in a manner that risks harming the organization, other users, or external parties, or that violates the requirements set out above.

User Account

Your user account is personal, and account credentials such as passwords and other equivalent codes and authentication devices (e.g. Microsoft Authenticator) shall be kept confidential in accordance with JU's password policy, see: (<https://ju.se/en/responsibility>).

You are only entitled to hold one user account. You have access to the account for as long as you are an active student at the University. An active student is defined as one where course or result registration has taken place within the last year. A student who has completed a degree without new registrations is regarded as an active student for up to six months from the date the degree was awarded. The University reserves the right to remove the user account and stored data when the student is no longer regarded as active in their studies.

You undertake to comply with this declaration of responsibility and the rules that supplement it. If you do not accept the rules, the account will be terminated.

Data shall be stored in accordance with the University's instructions in the document 'Recommended Data Storage at JU', available at (<https://ju.se/en/responsibility>). Your personal storage space in your home directory (G:) is limited and is dimensioned based on the needs arising from your education.

You undertake to regularly read your email.

SUNET's Ethical Rules

In order to use the University's computer, network, and system resources, you undertake to comply with SUNET's (Swedish University Computer Network) ethical rules: (<https://www.sunet.se/om-sunet/>). SUNET's principal task is to provide Swedish universities and higher education institutions with national and international data communications.

SUNET condemns as unethical when someone:

- attempts to gain access to network resources or other IT resources without authorization
- attempts to disrupt or interrupt the intended use of networks or connected IT resources
- attempts to damage or destroy computer-based information
- manifestly wastes available resources (personnel, hardware, or software)
- intrudes on the privacy of others
- attempts to insult or degrade others

Examples of Unethical Activity:

- attempts to alter or bypass system configuration
- installing software
- attempts to circumvent quotas
- obtaining unauthorized system privileges
- misuse of system resources
- unlawful distribution of copyrighted material
- sending unauthorized mass mailings see: (<https://ju.se/en/responsibility>)

Information to Users

Processing of Personal Data

Your personal data will be processed in the University's IT systems and services. For more information, see the Privacy Policy and information on personal data processing for the shared login service: (<https://ju.se/en/responsibility>).

Handling of Log Data

Continuous collection and follow-up of logs takes place regarding IT systems and services within the University and may be retained for up to two years. Follow-up is carried out for the purposes of:

identifying, preventing, detecting, and counteracting security incidents that may harm shared IT systems/services and/or the reputation of the University

for troubleshooting purposes, identifying and preventing operational disruptions in the University's shared IT systems/services

preventing and investigating security incidents where the University suspects that an employee, student, or external party has acted in violation of this declaration of responsibility or applicable laws

A system administrator is entitled, for operational security purposes and in the event of justified suspicion of violations of applicable rules and laws, to inspect an individual's stored data, programs, data communications, and other components related to IT operations.

Incidents

To enable communication with the account holder in the event of security incidents or password resets, it is important to provide verified private contact details in the self-service portal for user accounts: (<https://myaccount.ju.se>).

The University has limited computer resources. If a computer in a computer lab is left unattended for more than 20 minutes, others are entitled to log you out.

Instructions on how to terminate your account in advance (right to erasure), apply for an extension of the account's validity period, expanded storage space, and more are available via IT Helpdesk.

Deletion

Two months after the validity period has expired, the user account will be deleted. If the account holder has requested early termination, i.e. the right to erasure, the account will be deleted without delay.

Sanctions

Security incidents and violations of this declaration of responsibility and associated regulations may result in restrictions regarding the functionality of the user account in order to minimize the risk of harm. If the University has access to verified private contact details, the account holder will be notified of the incident. Otherwise, it is incumbent upon the account holder to contact IT Helpdesk.

IT Helpdesk decides whether the account can be restored or whether the matter shall be referred to DAN (the Disciplinary and Expulsion Board at the University). In the event of serious or repeated violations of this declaration of responsibility, the matter is always referred to DAN. Restoration of the account where the matter has been referred to DAN may take place no earlier than when the matter has been formally referred. If the account holder has acted in violation of applicable laws, the University may report the incident to an external party.

Miscellaneous

This declaration of responsibility is supplemented by rules available at (<https://ju.se/en/responsibility>). You undertake to keep yourself informed of changes to this declaration of responsibility and its associated rules. Changes are announced at least two weeks before they enter into force.