TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

Rules for the use of information systems

Turku University of Applied Sciences, April 16th, 2025

The aim of these rules is to secure a safe and comfortable study and work environment where information security and privacy can be guaranteed, and where the unhindered progress of studies and uninterrupted services of Turku University of Applied Sciences can be ensured.

Summary

The information systems and datasets owned or managed by Turku University of Applied Sciences (hereinafter referred to as the university) must be used and handled with care, and they must not be intentionally disturbed or damaged.

Usage must be related to studying at or working in or holding a position in the university or the student union, or to the performance of other tasks closely related to the university. Additionally, private use is permitted within the limits set in these rules. These rules can be supplemented with additional, more specific rules. Any other use requires a written permission.

Information systems must not be used with other people's user IDs. Personal passwords, PIN codes or other personal access keys must not be disclosed to others.

Unauthorised search for information security weaknesses and deficiencies, unauthorised connection of one's own information systems and services to the network or domain name (such as turkuamk.fi) and use of information systems without granted access rights are prohibited.

Private information should be clearly marked as private. It is the user's sole responsibility to transfer it elsewhere before the usage rights to any system expire. The university is not obliged to restore or deliver data retrospectively.

Privacy, copyrights, and license agreements must be respected.

Serious deficiencies and deviations in information security must be reported.

Inappropriate behaviour towards others is forbidden.

The binding rules can be found after the table of contents. At the end, there is a glossary to explain the terms. Feedback and questions can be submitted through our service portal.

Table of contents

Scope

These rules apply to the use and maintenance of information systems owned or managed by or otherwise under the responsibility of Turku University of Applied Sciences. The rules are also applied, where applicable, to such IT services for which the user has been granted access rights based on employment or position or right to study, or otherwise through the university.

The rules are binding on the staff of the university and students enrolled in degree education and, as terms of use, on all those to whom the university has granted access rights to its information systems.

Purpose and legal basis

These rules are a given in accordance with section 31 of the Universities of Applied Sciences Act (932/2014), which promotes internal order, the unhindered flow of studies and the safety and comfort of the university of applied sciences community. These rules protect information security of systems, privacy and the uninterrupted continuation of the services of Turku University of Applied Sciences.

Entry into force and updating the rules

These rules will enter into force on April 16th, 2025, by a decision of the Rector and President. These rules will replace the previous Rules of Use of Information Systems and the Rules of Use of Cloud Services. Policies and instructions guiding data processing, as well as more detailed instructions, rules and terms of use specific to devices, datasets, services or information systems, are issued separately. Turku University of Applied Sciences reserves the right to amend these rules of use. Users will be notified of the changes in the intranet Messi. The rules are maintained by the university's IT Services unit.

General rules for the use of information systems

User Responsibilities

Responsibility for datasets

- The user is responsible for the appropriate use of the datasets released for their use in accordance with the instructions and regulations given.
- The materials must not be broken or otherwise damaged intentionally or with gross negligence.

Responsibility for actions taken with your own username

- The user is responsible for all actions made using their username and for any damage caused, unless otherwise provided by law.
- The user's liability for additional damage caused by their user account ends when the user has notified Service Desk that their account may have been compromised by another person.

Responsibility for personal private information

- The university is not responsible for the preservation or security of personal private information stored in its systems, but the owners must take care of it themselves. If the user's access to the information system expires, the user must transfer their private data in time. The university is not obliged to return data retrospectively.

Obligations of the User

Regulatory compliance

- The user must comply with these rules of use and other regulations of the university, such as community rules, policies and instructions guiding data processing, as well as more detailed instructions, rules and terms of use specific to devices, datasets, services or information systems.

Protecting Your Credentials

- Your username password, PIN code or other personal access key must not be disclosed to others.

- If you suspect that your password, PIN code, or other personal access key has fallen into the knowledge or possession of someone else, its use must be blocked, or it must be replaced. The matter must be reported in the service portal without delay.

Marking up private material

- To ensure the protection of privacy, users must keep their private material clearly separate from other material and mark it. A student's emails and instant messages are always considered private. However, this does not prevent the automated technical monitoring of information security permitted by law.

Taking care of data protection

- Personal data and information that is confidential under the law, or information provided at the discretion of the university must be handled carefully and in accordance with the instructions given. This also applies to all information marked as confidential or secret.
- The user has a duty of confidentiality regarding data content, uses, security level and features of information systems when required by law or usage rules, or when it is obvious that the disclosure of information would endanger the systems and cause harm, damage or danger.

Obligation to report deviations

- Detected or suspected serious deficiencies and deviations from information security must be reported.
- If you come into possession of messages or other information belonging to others, you must notify the owner of the information, or Service Desk through the service portal, so that confidentiality of communications can be ensured. Do not attach the data itself to the report.

Permitted use

Use for studying and carrying out assignments at the university

- Usage must be related to studying at or working in or holding a position in the university or the student union, or to the performance of other tasks closely related to the university. Additionally, private use is permitted within the limits set in these rules. These can be supplemented with additional, more detailed rules. Any other use requires written permission.
- Systems must be used in accordance with their intended use and license agreements.

Use for private purposes

- Your own privately owned devices can be connected to the university's network in the parts of the network intended for this purpose, following the instructions given by the university.
- The private use of the university's information systems is allowed if it does not interfere with other use and does not violate the law or more detailed instructions, rules and terms of use given.

Prohibited Uses

Use without valid authorisation

- The use of the university's information systems without a valid user authorisation is prohibited.

Use contrary to laws and good practice

- The information systems may not be used in violation of European Union regulations or Finnish laws, decrees and official regulations.
- Behaviour that is likely to cause harm or suffering to others is prohibited. This includes threats, defamation, continuous disruptive messaging, harassment and disclosing details of other people’s private lives or information.

Use in violation of license agreements

- License agreements must be adhered to. Computer programs or materials must not be used or distributed in the university's networks or devices in violation of the licence agreements.

Interfering with information systems and unauthorized intrusion attempts

With the exceptions provided below the list,

- Information systems must not be deliberately overloaded or otherwise deliberately disrupted. Denial-of-service attacks are prohibited.
- It is prohibited to capture, disclose or exploit confidential messages or information addressed or belonging to others.
- Copying or modifying telecommunications is prohibited.
- Unauthorized decryption or attempted decryption is prohibited.
- It is prohibited to look for weaknesses and deficiencies in information systems by means of vulnerability scans or other technical methods which could be exploited to access systems without permission or to find out or change the information content, properties or functions of the systems without permission. This does not prevent reporting of observations made during normal use.
- Parts or features of information systems that are not clearly made available for public use, such as maintenance tools or functions blocked by system settings, may not be used without permission.

Activities related to the university's operations are allowed when they are carried out in accordance with the unit's plans. The university's management, information security officer and IT Services have the right to carry out, or commission, planned information security testing for the entire university.

Systems and services connected to a network or domain name without permission

- Devices, services or other systems that control or interfere with data traffic may not be connected to the university's public network, unless a separate permission has been obtained from IT Services.
- Services publicly visible on the Internet must have the permission of the domain name owner.

Management of access rights to information systems

Decisions on access rights are made by the university

- User rights are managed in accordance with separate system administration rules.
- As a temporary measure, the university has the right to restrict such use of networks or information systems that jeopardise data processing, or if it detects or suspects a violation of the rules.

Revoking access rights

- The authorisation to use the licence is cancelled if it is manifestly unfounded, or if the grounds for granting it, such as the right to study, employment relationship, position of trust or other special grounds, cease to exist, or if the new duties no longer require the same authorisations to use.
- Accounts that have been unused completely or for long can be closed after a specified period to minimise unnecessary access rights.
- After the termination of the right of use, the university is not obliged to store the user's personal private files and messages, but these can be deleted, and the university is not obliged to restore them afterwards.
- User rights can be revoked for a fixed period due to a violation of the rules.

Monitoring and security measures

- The university has the right to supervise compliance with these rules and to protect the information security of its information systems (links to legislation in Finnish language version).
- Information systems can be monitored automatically. To protect information systems, automatic restriction, blocking and isolation measures can be taken in this context.
- The supervisory responsibilities for data protection and information security are defined in the information security policy.

Vocabulary

User
A person or device or IT process that has been granted access rights.

User ID
An identifier that identifies the authorized user of the information system.

Access rights
Rights granted to a person, device or IT process to use a specific information system to perform its tasks. Access rights can be granted as a user ID or by allowing access from certain web addresses, at a certain time, with a different access criterion, or a combination of these.

Main or supervisory user and (technical) administrator
A person who manages the information system and its access rights and user IDs on behalf of the owner and who may have the opportunity or obligation to monitor the activities of other users in the system.

Information system
An overall arrangement consisting of data processing equipment, software and other data processing. For example:

1. wireless and wired telecommunications networks managed by the university
2. data processing equipment connected to the university's network
   (such as computers, Audio-Video systems or printing systems)
3. software and services that work in the previous [1,2]
4. Infrastructure, platform or application services delivered by or through the university
   (such as services used with a web browser: virtual desktops and servers, webhosting, Microsoft 365, Adobe Creative Cloud etc.)
5. the data content of the systems mentioned in points 1 to 4 above

The (administrative) owner of the information system
The party for whom the system has been acquired and who determines who is entitled to use the system.

Information security
Maintaining the confidentiality, integrity and availability of information. Confidentiality means that the information is only available to the desired parties. Integrity means, among other things, correctness, completeness and timeliness. Availability is the process of getting information at the right time in a usable and understandable format and quickly enough.

Information security incident
Compromise or loss of information security. For example, malware, phishing messages and web pages, compromised confidential or secret information, lost computer or storage device, service outages, data breaches, or espionage.

RDI activities
Research, development and innovation activities.

Domain Name
A portion of the website address and email address that identifies the service provider. Turku University of Applied Sciences' domain names include, for example*, turkuamk.fi* and other domain names acquired for special needs.

Version history

Date	Change	Decision by
13.9.2005	Rules for the use of information systems have been updated (based on a date in the document).	No digital record
18.5.2015	The rules of use of cloud services are given.	Director of Services Sami Savolainen
25.5.2015	Cloud access rules reviewed (date in document).	No digital record
1.2.2016	Cloud access rules reviewed (date in document).	No digital record
22.2.2022	The rules for the use of information systems have been revised. Rules dated 10.2. Minutes of the decision 22.2.	Service Manager Mika Suutari, Learning Environment Services.
16.4.2025	New rules for the use of information systems have been issued as a regulation in accordance with the UAS Act. The new rules will repeal the old rules and the rules for the use of cloud services.	Rector and President Vesa Taatila.

The rules for the use of cloud services have been included in the version history, as they have been repealed by these rules. These rules have been discussed by the Advisory Board on Co-operation on 7 April 2025.