Rules of IT Service Use

University of Tampere
University services / IT Administration

Rector's decision 28 August 2014.

Table of contents

1 Scope

IT services refers to all IT systems and hardware provided by the university, including services made available or authorised by the university.

The Rules of IT Service Use apply to all use of the university's IT services.

2 Usage authorisation and user ID

2.1 Usage authorisation

Usage authorisation refers to the user's authority to use a particular service. The usage authorisation is verified every time the service is used.

The scope of usage authorisations depends on the user's status and role. Users may be authorised upon personal request, and the authorisation may have a fixed expiry date. Usage authorisations may change as the user's status or role changes.

2.2 User ID

Unless the authority to use the service has been granted to all Internet users, the user must be identified reliably enough to ensure appropriate usage authorisation. This is done with the user ID and password or by another means of identification.

Compliance with these Rules of IT Service Use is a prerequisite for receiving a user ID.

A definite group of users may be granted a joint user ID, a group ID, which features the usage authorisations of the group members. Group IDs are used for the specific purpose they are granted for and they are valid for a fixed term.

The user applying for a group ID is responsible for distributing the ID to other group members and changing the password, as necessary.

Group IDs may only be used for the purpose they were granted for.

2.3 Each user is personally responsible for their user IDs

User accounts must be protected using strong passwords or according to other instructions. If there is reason to believe that a password or another identifier has been compromised, the password must be changed or the use of the identifier prevented immediately.

User accounts and their passwords may never be given to another person.

Each user is responsible for all actions conducted using his/her ID. The responsibility also applies to situations where the ID is used by a party that received the necessary information and tools from the user, whether on purpose or by negligence.

The use of another person's user ID is forbidden, even upon the user's own request.

Each group ID user is responsible for his/her actions conducted using the ID.

The group ID may not be given to non-group members.

2.4 Expiry of usage authorisations

All usage authorisations expire when the person is no longer a member of the university community.

An individual usage authorisation expires when

- the granted fixed term usage authorisation expires or
- the person's role changes, and the new role does not make them eligible to use the IT services.

A user must save all private e-mails and files he or she will need from the system before the expiry of the IT service usage authorisation. University staff members must transfer all work-related messages and files to the person agreed upon with the supervisor. This also applies to students who have worked in research teams or similar activities.

All users must uninstall any software based on employee or student licenses from their home computers when their employment or study right ends.

3 Users' rights and responsibilities

3.1 The IT services are intended for work- and study-related use

The University’s IT services are intended to serve as tools for tasks related to studying and working at the university.

Publishing, forwarding or distributing material that is against the law or good practice is prohibited.

3.2 Information security is everyone's responsibility

Any detected or suspected breaches or vulnerabilities in information security must be immediately reported to the IT Administration customer service.

Personal passwords must never be disclosed to anyone.

Everyone is obliged to maintain the secrecy of any confidential information that they become aware of.

The phishing, abuse, copying and distribution of other users' private information is forbidden.

The university is entitled to restrict or revoke the right to use its IT services as a precaution.

3.3 Small-scale private use is allowed

Small-scale private use refers to such actions as private e-mail conversations and online service use.

However, private use must never disturb other use of the system or breach the rules and instructions of IT service use.

3.4 Everyone is entitled to privacy

All materials that are in students' possession are deemed to be private.

Staff members must clearly separate their private materials from work-related ones. This rule also applies to students working for the university.

3.5 The university may restrict the use of the communications network

The university's IT Administration has the right to restrict the devices that can be connected to the university's communications network. Usage can be restricted by technical or instructive means.

Services may not be provided using the university's network without the university's permission.

3.6 Bypassing information security mechanisms is forbidden

Usage authorisations must never be used for any illegal or forbidden activities, such as searching for vulnerabilities in information security, unauthorised decryption of data, copying or modifying network communications, or unauthorised access to IT systems.

Parts and features of IT systems that are not clearly made available for public use – such as system administration tools or functions prevented in system settings – must not be used.

4 Other provisions

4.1 Exceptions from the Rules of Use

Permission for exceptions from the Rules of Use can be granted for compelling reasons upon a written application. Permits for minor exceptions are granted by the Chief Information Officer. The permit may include additional terms and conditions, restrictions and responsibilities.

4.2 Monitoring and consequences of breaches

Compliance with the Rules of Use is overseen by the IT Administration, owners of services and IT services, as well as supervisors.

The consequences of breaches to the rules of use are decided upon by the Rector or a person appointed by the Rector.

The consequences can be disciplinary or legal, and they are determined by the Criminal Code, the Employment Contracts Act, the Universities Act, the University Regulations and the provisions based on them.

4.3 Validity

These Rules of IT Service Use become effective on 1 September 2014 and replace the earlier version of the corresponding rules.