Rules of IT service use in brief

These binding rules concern all users. Including you.

These rules apply to the use of all of the University's IT services, hardware, software and networks.

The University authorises users to access its IT services by granting user IDs (user accounts) or making services available.

Every user is personally responsible for all use of the services with his/her user ID.

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

They may also be used for personal purposes within reason and in keeping with laws and good practices.

Other users' privacy and ownership of information must be respected at all times.

Use of the services for any commercial or propagandistic purposes is forbidden.

Unauthorised use is forbidden.

Use of services is monitored, and breach of these rules will be sanctioned.

Further specifications to these rules are provided below.

Rules of IT service use

The Rules of IT Service Use bind and obligate all members of the university community, users of IT services and systems, and all units of the University. These rules apply to all of the University's IT services and hardware, and the use thereof, also including services made available or authorised by the University. Examples of such services are CSC's services HAKA, Funet, etc. Tampere university of technology rules and recommendations call all these as IT services.

These rules bind and obligate all members of the university community as well as other users of IT services and systems regardless of the ownership of the devices or the systems used for accessing these services.

In TUT the design, implementation as well as operations security is based on the best practices and instructions made available by The Government Information Security Management Board (VAHTI). In case there is a need to deviate from these instructions and practises it is done by documented reasons.

Usage authorisation

Usage authorisation is granted by issuing a user ID or making the service available.
Authorised users are allowed to use the university's IT services. Compliance with the Rules of IT Service Use is a prerequisite for authorisation.

- The scope of usage authorisation depends on the user's status and tasks (roles) at the University
- one person may have several roles

Usage authorisation is granted for a fixed term
The authorisation expires when
- the person is no longer a member of the university community
- the granted fixed term user ID expires
- the person's role changes, and the new role does not make him/her eligible to use the IT services.

Usage authorisation can be restricted if there is justified reason to suspect that information security has been compromised or the services have been abused.

The access rights are closed after 7 days of the expiration of the usage rights, also receiving emails to TUT managed address will be prevented. The user must remove all personal e-mails and files from the system before the expiry of his/her usage authorisation. The University will delete all files and mailbox contents when 3 months have passed since the expiry of the user ID or usage authorisation. University staff members, as well as students who have worked in research teams or participated in other such activities, must transfer all work-related messages and files to the person specified with the supervisor.

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

User ID

- Users are identified (authenticated) with the user ID (user account)
- every user must have an individual ID for all IT services that require authentication.

Group IDs can be granted upon request for special purposes
The use of group IDs can compromise the confidentiality of information. For example, in the case of using an administrator-level group ID in order to use special software in a computer lab.
- The user who applies for a group ID is responsible for the distribution of the ID
- group IDs may only be used for the purpose specified in the application and granted permit
- every group ID user is responsible for his/her actions conducted using the ID.

Every user is personally responsible for his/her user IDs
User accounts must be protected using strong passwords and complying with other instructions. If there is reason to believe that a password or other account details have been compromised, the password must be changed or the use of the compromised element must be prevented immediately.
- Never dispose or lend your username and password to other persons
- each user is responsible for all actions conducted using his/her ID
- users are financially and legally liable for any damage or loss caused using their ID
- the use of another person's ID is forbidden, even upon the user's own request.

Users' rights and responsibilities

The IT services are intended for work- and study-related use
The University's IT services are intended to serve as tools in tasks related to studies, research, teaching or administration.

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
- breach the rules and instructions of IT service use.

Commercial or propagandistic use is not allowed
Special permission for these purposes can, however, be applied from IT management.

- Commercial use is only allowed in cases assigned by the University
- use for pre-election campaigns or other political activities is only allowed in conjunction with the University's elections and activities of the Student Union, student organisations or trade unions
- all propagandistic use is forbidden
- unnecessary consumption of resources is forbidden.

Laws must be observed

- Material that is illegal or against common manners must not be published or distributed.

Everyone is entitled to privacy
The right to privacy, however, does not cover all work-related material that is in an employee's possession.

- All materials that are in students' possession are deemed to be private
- staff members must clearly separate their private materials from work-related ones
    - e.g. create a directory entitled "Private" or "Personal"
    - this rule also applies to students working for the University.

Information security is everyone's responsibility
Any detected or suspected breaches or vulnerabilities in information security must be immediately reported to TUT security specialist, system administrator or according to other given instructions.

- Personal passwords must never be disclosed to anyone
- everyone is obligated to maintain the secrecy of any confidential information that may come to one's knowledge
- abuse, copying and distributing other users' private information is forbidden.

As a precaution, the University is entitled to restrict or revoke the right to use its IT services.

Setting up unauthorised services is forbidden
Only devices approved by the University may be connected to the IT network. Only services authorised by the University may be produced using the university's IT networks.

Bypassing information security mechanisms is forbidden
Usage rights 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.

Phishing for information and deceiving users is forbidden
Cheating and unauthorised acquisition of information is forbidden.

Other clauses

Validity
These rules of IT service use become effective 1.8.2013 and replace the earlier version of corresponding rules. After the date specified above, all new IT services must be produced according to these rules.

Change management
These rules will be reviewed when needed to ensure that they comply with all valid services and laws. Any significant changes to these rules are addressed according to the co-operation procedure. The head of Information management makes decisions concerning change needs.

Information about changes is distributed using the regular communication channels, never personally.

Exceptions from the rules of use
Permission for exceptions from the rules of use can be granted for compelling reasons upon a written application. Exceptional permits are granted by the head of information management. The permits may include additional terms and conditions, restrictions and responsibilities.

Monitoring
Compliance with the rules of use is overseen by the IT department, owners of services and IT services, as well as supervisors within their job descriptions. Breaches of the rules lead to sanctions according to the consequences of IT service abuse documentation.