LUT UNIVERSITIES

IT Service Use Policy

IT Service Use Policy

IT Service Use Policy of LUT Universities binds and obligates all members of the LUT Universities community, users of its IT services and systems, and all units of the higher education institutions of LUT Universities. The policy applies to the use of devices and IT services provided by your higher education institution and the use of services authorised or enabled by your higher education institution.

Access rights

Access rights are granted by issuing a user ID or making a service available. If you are an authorised user (hereninafter user), you may use your higher education institution's IT services. Access rights require compliance with this IT Service Use Policy.

- The scope of your rights depends on your position and job duties (roles).
- You may have several roles simultaneously. When you are acting in a specific role, employ the user ID connected to that role. For example, if you are both a student and an employee, use your employee ID for your job duties.

Access rights are granted for a fixed term

Your access rights expire when

- you are no longer a member of the higher education community
- your fixed-term user ID expires
- your role changes and your new role does not make you eligible to use IT services.

Access rights can be restricted whenever the university considers it necessary. You must remove all personal emails and files from the system before your access rights expire. If you are a staff member, transfer all necessary messages and files to a person approved by your supervisor. This also applies if you are a student but have worked in e.g. a research group. 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 a user ID.
- Every user must have an individual ID for all IT services that require authentication.

You are personally responsible for all of your user IDs

- To protect your user accounts, you need to use strong passwords and comply with other instructions. Follow separate instructions on how to choose a good password.
- Never give your username and password to another person.
- You are responsible for all activity using your user ID and are liable for any damage or loss caused using your ID as a result of either a wilful act or negligence.
- You are never allowed to use another person's user ID.
- If you have reason to believe that your password or other identifiers have been compromised, change your password or prevent the use of the identifier immediately.

Users' rights and responsibilities

IT services are intended for work and study

IT services are meant to help in studies, teaching, research or administrative duties.

Small-scale private use is allowed

Small-scale private use refers to such actions as private email correspondence and use of online services. However, private use must never

- disturb other use of the system
- breach the policies and instructions of IT service use.

Use for commercial activities or propaganda is not allowed

- The commercial use of IT services is only allowed in cases assigned by your higher education institution.
- Using IT services for election campaigning or other political activity is allowed only in internal elections of your higher education community and in internal activity related to the student union, student associations and higher education community to a separately specified extent.
- All propagandist use of IT services is forbidden.
- Do not use IT service resources unnecessarily.

Laws must be observed

- Do not publish or distribute material that is illegal or contrary to good practice.

Everyone is entitled to privacy

The right to privacy does not, however, 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 and interns should keep their private materials clearly separate from work-related materials (e.g. a folder named “Private”).

Information security is everyone's responsibility

If you detect or suspect any breaches or vulnerabilities in information security, report them immediately to security@lists.lut.fi.

- Never disclose your personal passwords to anyone.
- You are always obligated to maintain the secrecy of confidential information that comes to your knowledge.
- Abuse, copying and distributing other users' private information is forbidden.
- As a precaution, the higher education institutions are entitled to restrict or revoke the right to use their IT services.

Do not set up unauthorised services

You may only connect devices approved by your higher education institution to the institution's IT network. You may only produce services authorised by your higher education institution using the institution's IT networks.

Do not bypass information security mechanisms

Never use your access rights 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. Do not use parts or features of information systems that are not explicitly offered for general use. This includes, for instance, maintenance tools or actions prevented with system settings.

Phishing for information and deceiving users is forbidden

Deception and unauthorised acquisition of information are forbidden.

Other clauses

Entry into force

These rules have been approved by the chief information officer and will enter into force on 15 February 2021. This policy will replace the previous equivalent rules. Users are obligated to follow the IT Service Use Policy in force.

Amendments

This policy will be reviewed regularly to ensure that it complies with all valid services and laws. Any significant amendments to this policy will be addressed according to the co-operation procedure. Information on amendments will be available through the communication channels of the higher education institutions. Everyone is obligated to read the amendments.

Exceptions

Permission for exceptions to the IT Service Use Policy can be granted for compelling reasons based on a written application. Permission may be granted by the chief information officer. The permission may include additional terms and conditions, restrictions and responsibilities.

Monitoring

Compliance with the IT Service Use Policy is overseen by Information Services and Technology, owners of services and IT services, and supervisors with regard to their teams. Breaches of the policy lead to sanctions according to the Sanctions for IT Service Abuse.

Lappeenranta

Antti Sirviö
Chief Information Officer

Tämä dokumentti on allekirjoitettu sähköisesti LUT Sign-järjestelmällä
This document has been electronically signed with the LUT Sign system

Päiväys / Date: 10.02.2021 10:20:41

Antti Sirviö

LUT University
Antti Sirviö
Tietohallintojohtaja

Organisaation varmentama (LUT käyttäjätunnus)
Certified by organization (LUT user account)