Graubner, Pettinen, Valjakka

17 February 2021

Regulations for the use of IT services at Laurea

Discussed at the codetermination advisory board of Laurea University of Applied Sciences on 17 February 2021

Graubner, Pettinen, Valjakka 17 February 2021

Table of contents

Graubner, Pettinen, Valjakka

17 February 2021

1 Scope of rules

Laurea has a duty to ensure the availability, confidentiality and integrity of information needed in Laurea's operations by all users and user groups belonging to the community, and to provide a reliable and secure environment for processing information. Laurea also has a duty to enable the students' smooth progress in their studies, ensure equal supervision and treatment, and minimise misuse.

These and other regulations are designed to help users belonging to different groups to identify the rights, responsibilities and obligations associated with their user rights. Neglecting the duties related to user rights, even unintentionally, may endanger the integrity, confidentiality and usability of information owned by other users.

These regulations apply to all information systems under Laurea's control or otherwise under the responsibility of Laurea, and their use, as well as other services that have been granted access to or authorised through Laurea. The regulations also apply to workstations in general use at Laurea and all devices connected to Laurea's network.

In addition to valid legislation, all IT users at Laurea must comply with these and other regulations and instructions followed at Laurea. The use of these or other information systems contrary to the regulations is handled in accordance with the Sanctions policy for the misuse of IT services at Laurea.

The latest effective versions of user regulations and other information security regulations are published on the website of IT Management services in the intranet.

2 Updating the regulations

User regulations are regularly reviewed at Laurea to correspond to changes in services or legislation. IT Management is responsible for the monitoring and updating.

3 General principles

Activities in violation of this instruction or other policies and guidelines concerning the use of the information system may result in a temporary or permanent closure of user rights.

Key principles guiding all usage and interpretation of the user regulations include:

- All authorised persons have the opportunity to use the services in a reasonable and appropriate manner.
- No damage or harm shall be caused to the equipment, information systems, users or data in the telecommunications network.
- Privacy must be respected.
- The usage shall take place in conformity with the regulations in force and be ethically acceptable.
- The publication, transmission and distribution of material that is unlawful or contrary to accepted principles of morality, and the unnecessary loading of system resources are strictly prohibited.

- Equipment provided by Laurea to its staff for the completion of work tasks must not be made available to third parties, such as family members.

4 Restrictions on use

Information systems at Laurea are intended to be used as tools for tasks related to studies, research, teaching or administration at Laurea University of Applied Sciences. Other usage requires a separate agreement, such as a research permit.

The use of Laurea's information systems or user IDs for political activities is prohibited. Permitted exceptions include the elections of the Student Union Laureamko and union activities of staff, or similar. Commercial use other than on behalf of Laurea is only permitted under a separate authorisation.

5 Private use

Minimal private use is allowed and only to the extent that it does not

- harm Laurea's information systems or data included in them, equipment, or users
- create a need for making changes to Laurea's computing environment
- conflict with the regulations and guidelines for individual systems or general use.

Sending and forwarding of circular e-mails, ads, spam, e-mails involving money collection or similar content is prohibited.

Laurea's email address shall not be used for registering to services other than those related to work or studies.

Private material must be kept clearly separate from material related to Laurea's basic operations. Material in the student's home directory is always considered private.

To ensure their personal privacy, staff is advised to keep private material clearly separate from work-related material. Private material must be stored in personal folders and named so that the privacy is clearly visible (such as personal, private or private matters).

6 User responsibilities

For their part, all service users are responsible for the overall safety of Laurea's information systems and data contained in them, and for using the information only for the purposes of their task/role.

- It is forbidden to acquire, use or attempt to access information in the information systems. For example,
  - creating lists or registers of users of IT services at Laurea, or their data
  - searching for and reading confidential information and files
- If the user accidentally receives information addressed to or belonging to others, its exploitation, recording and distribution are prohibited. Such occurrences shall be reported to the system maintenance personnel and/or the

user concerned, and a safety report shall be filed in the intranet (Information Society Code 917/2014).
- It is forbidden to use the right of access to search for security vulnerabilities, unauthorised decryption, tracking, copying or changing communications, or intrusion into other systems, directories, or services.

All users shall, for their part, take care of matters related to shared information security. This also applies to the protection of your own privacy.

Information security deficiencies and misuse that have been detected or suspected must be reported without delay in accordance with the instructions given.

Laurea aims to protect all users from malware, spam and attempts to intrude into the systems or individual workstations. For their part, the users shall also take care of information security by following the instructions given (intranet/IT Management/IT security and protection).

In online teaching situations where the competence of the identified student needs to be reliably and genuinely verified, separate monitoring methods can be used in accordance with the data protection principles specified for online teaching. User IDs are required to be used in accordance with the instructions provided in the systems used for online teaching.

IT Management is responsible for backing up Laurea's shared information systems and their data. In addition, Laurea offers the opportunity to back up users' files (OneDrive), but is not responsible for any damage caused by the possible destruction of files. The users are ultimately responsible for classifying their own data and for backing it up.

The users are bound by the obligation of professional secrecy regarding the data content, usage, protection methods and properties of the systems.

7 Connecting to Laurea's information network

Only devices owned by Laurea and approved and registered by the network administrator may be connected to Laurea's internal communications network. When connecting devices to the network, instructions given by IT Management must be followed. A separate wireless network is reserved for visitors' personal devices. Physical network connections are always handled by Laurea's IT Management (such as workstations).

8 User rights and user IDs

User rights and user IDs shall be implemented independently using strong identification. For users who cannot be identified electronically, a staff member of Laurea checks the identity when handing over the user ID.

The users are granted rights to use Laurea's shared information systems. The user right is based on the position of the user in Laurea. If necessary, it can also be granted to a person who is not a student at Laurea or a member of Laurea's staff, such as visitors. Visitors may be granted limited access to computers in shared use in Laurea's premises.

Access to systems in restricted use is granted separately on a case-by-case basis.

A prerequisite for user rights is that the user undertakes to comply with these regulations and other usage instructions and rules. The users must familiarise themselves with the operating instructions and regulations applicable to the system in advance.

- Users are personally responsible for the harm or damage caused by the use of their account ID.
- Identity falsification and the use of another person's ID are prohibited.
- Access rights are personal and must not be shared.
- If there is reason to suspect that someone else knows your password, the password must be changed. Contact Laurea's Service Desk without delay (tel. +358 9 8868 7112, servicedesk@laurea.fi) to prevent the use of the account ID, and to file a safety report.
- Change your password regularly and make sure it is sufficiently complex. IT Management urges you to change your password at regular intervals in accordance with practices in force at a given moment (see chapter 11 for instructions).

9 Validity of user rights

The user rights expire:

- when the user is no longer in an employment or study relationship with Laurea
- when a fixed-term licence expires or
- when the position of the user changes so that a licence to the information system in question is no longer justified.

The user ID is terminated when

- the user rights, to which it is assigned, end
- there is no longer a need for it
- there are reasonable grounds to suspect that it has been misused or information security has been compromised
- Measures required before the termination of user rights:
- To ensure the continuation of the work tasks, a member of personnel shall transfer the work-related messages and files as necessary to a person agreed in advance with the supervisor. This also applies to students who have worked in research groups or similar.
- Users must ensure that the information owned by their user ID is appropriately transferred or deleted.

User ID files stored in the information systems shall be deleted no later than 12 months after the expiry of the user rights.

10 Legislation on the use of information systems at Laurea University of Applied Sciences

- Archives Act (831/1994)
- Act on the Openness of Government Activities (621/1999)
- Act on the Protection of Privacy in Working Life (759/2004)
- The Criminal Code of Finland (39/1889, Chapter 35, Sections 1 and 2; Chapter 38, Section 2, Chapter 38, Sections 3–4; Chapter 38, Section 8)
- The Constitution of Finland (731/1999, Sections 10–12)

- Copyright Act (404/1961)
- Act on Universities of Applied Sciences (932/2014)
- Data Protection Act (1050/2018)
- General Data Protection Regulation (EU) 2016/679
- Information Society Code (917/2014)
- Act on Information Management in Public Administration (906/2019)

11 Instructions

- Classification of data
- Security and Data Protection Guidelines

12 Appendices

- Regulations for the use of IT services (PDF)
- Sanctions policy for the misuse of IT services