02/2016, Director of Administration

User rules of the Laurea IT Management

1 Operating principles

- The rules apply to every user.
- The rules apply to any use of Laurea’s IT-service (devices, software, data and information system).
- Laurea appoints user access authorization by granting a user account and bringing the service available for use.
- Everyone is personally responsible for all the use of their user accounts.
- IT-Services are intended for work tasks and studies.
- If the person with user access rights of the IT services follows moderation, laws, good manners, he or she is allowed to use the services also for taking care of private matterin minor volume at his or her own risk. The user is responsible for this private use. Laurea is not responsible for the functionality or accuracy of IT services or possible damage caused in connection to using the service for private purposes.
- Everyone needs to respect privacy and ownership of the information.
- All commercial and/or public advertisement actions for private matters is strictly forbidden.
- All unauthorized use is forbidden.
- Use of the services are monitored. Breaking the rules has it's consequences.

2 User rules of the Laurea IT-Services

The user rules of Laurea's IT services apply to and obligate all users of Laurea's IT services and information systems.

The rules apply to all devices and IT services of Laurea as well as their use. The rules also apply to the services and user access rights for which access or user authorization has been granted by Laurea. These services include CSC services, such as HAKA and Funet etc. as well as user rights, such as access at home to the MS Office package provided by Microsoft.

Personal files and e-mails must be separated from work-related ones and stored in a separate directory clearly marked as 'personal'. Laurea is not responsible for maintaining or storing any per-sonal files, e-mails or other personal materials of users. Laurea is not responsible for any damage caused in connection with personal use, and under no circumstance is Laurea liable to compensate for any damage caused to the user's personal materials.

3 User access authorization

3.1 Admittance of user access authorization

User access authorization will be appointed by granting a user account and bringing the service available.

Only the authorized personnel are allowed to use the Laurea IT-Services.
It is a prerequisite for the user to follow the rules in order to utilise the authorization. All the authorization rights depend of the user's role in the Laurea organization. A user may have multiple roles at the same time.

3.2 Termination of user access authorization

User access authorizations are temporary. User access authorization ends, when:

- Temporary authorization expires.
- User's role changes to another role, which does not have a requirement for IT-service authorization.

3.3 Restriction of user access authorization
User access authorization can be restricted, if there is a reason to suspect deceit or a break in the information security.

3.4 Once the user access authorization ends
The user needs to remove his/her personal emails and files before the user access authorization ends.

Laurea removes the files and the mail inbox after a certain pre-determined time once the authorization has ended. If the user is a staff member, he/she has to transfer the job related emails and files to a designated person. (has to be coordinated with a superior). This also applies to a student, who has worked in a research project or group.

All staff- and student licensed software's for home use are to be removed from the computer once the employment contract or the studying right ends.

4 User account

The user is identified and authenticated with the account ID.

Every user must have their private account for IT-services, that require identifying. Separately requested group accounts are an exception. (see 4.1 below)

4.1 Group account can be granted by application for special purpose
Use of a group account can endanger the confidentiality of information.

Group account requestor is responsible for the sharing of the account.
Group account may only be used for the purpose it was granted for.
Every user of a group account is responsible for their own use of the group account.
Group account user access authorization is valid only for the requested time.

4.2 Everyone are responsible for their personal accounts
User accounts are to be protected with strong passwords. If a password is suspected to have been stolen, it has to be changed or the account has to be suspended immediately.

User account is your personal account, one cannot give it to another person.
The user is responsible for all the use on his/her account.
The user is responsible for any damage done by the use of his/her account
Use of other person's account is strictly forbidden, even if the other person would request it.

5 User rights and responsibilities

5.1 IT-Services are intended for work tasks and studies
Laurea IT-Services are intended to be tools and instruments for tasks regarding studying, working, teaching, research and administration in Laurea.

5.2 Private use is allowed in minor volume
Minor volume private use is for example: email conversations and use of network services. However the private use must not:

- Hamper the use of the service.
- Conflict with the rules and regulations of the service.

5.3 Commercial use or publication is not allowed as a private use
Use of Laurea IT-Services for political or other public use is only allowed in Laurea's internal elections. (Student Organizations and labor unions)
Unnecessary use of resources is forbidden

5.4 Obey the law
Releasing and sharing of illegitimate material is strictly forbidden.

5.5 Everyone have a right to privacy
However privacy doesn't cover every work related material in the user's possession.

- Student's materials are considered private.
- Staff personnel's private material has to be kept clearly separated from the work related material. This rule applies also to a student working for Laurea.

5.6 Everyone are responsible for information security
All encountered or suspected flaws and violations of information security are to be reported to the IT services or by filing a safety report at the Laurea intranet immediately upon notice. All encountered and/or suspected flaws and violations of information security are to be reported to the IT-Management immediately upon notice.

- Personal password must never be told to anyone.
- Everyone have a professional confidentiality of any and all confidential information they receive.
- Account information theft, exploitation, stealing and sharing is strictly forbidden.
- Laurea has the right to protect it's information security by restricting or blocking the use of IT-services.

5.7 Installing an unauthorized service is forbidden
You may install devices to Laurea information network only if they are approved by Laurea.

The only exception are the guest networks. Any user can connect any device they wish to the guest network in Laurea, no permissions required. If need be, the IT-Management informs of any restrictions to the guest networks.

Services can be produced in all Laurea's networks with the exact permission from the IT-Management. This applies to all networks.

5.8 Bypassing of security mechanisms is forbidden
None of the user access authorizations may be used to illicit or illegal actions.
Such actions include: searching for vulnerabilities, illegal encryption of security mechanisms, breaching the system or hacking the data.

Parts of the IT-Services, that are not publicly announced services cannot be used. Such services are for example: Administration tools or blocked features.

5.9 Information theft and user deception is forbidden
Don't cheat or obtain information illegally.

6 Other regulations

6.1 Ratification
These user rules of the IT services will enter into force on 1 January 2017 and will replace any previous relevant rules. After this date, new IT services will be implemented according to these rules.

6.2 Alteration management
These rules will be re-inspected so that they match the valid services and law.
Notable changes will be processed in co-determination. The Director of IT-Management will decide whether there is a need for change. The Director of IT services shall determine wheter there is need for change.

Information about the change will come through conventional information channels, not private.

6.3 Deviation from the user regulations
A permission to deviate from the user regulations can only be authorized by sending a written application and a reasonable plea. The permission to the deviation may be granted by the Director of IT Services. There can be conditions, regulations and additional responsibilities in the given permission.

6.4 Monitoring
IT-Management observes and monitors that the rules and regulations are followed. Service owners and managers are also responsible for monitoring in case of foul play. Violations will be punished according to information security policy.

6.5 Additional information
Other rules and guides regarding the use of Laurea IT-Services can be found from Laurea intranet. References mentioned in this rule-document can be found at the Laurea intranet.

Laurea's IT maintenance personnel monitor compliance with this Code of Use and will answer questions related to it on, Contact information.

Laurea University of Applied Sciences
IT Management

I accept user policy

Date: _____

Signature: _____

Name: _____