Central Services
IT Services

Lucerne, 31.05.2010 / 14.08.2013

Translation of the document dated 31.05.2010 (signed on 1.06.2010; version 1.26)

Terms of Use for IT Resources

Instructions for the use of IT resources at the University of Lucerne

1 Section I: General Provisions

1.1 Purpose

These instructions govern the use of IT resources at the University of Lucerne.

Their purpose is to protect the sensitive stored data, ensure the secure and economic use of the IT resources as well as to preserve the personal rights of the users.

1.2. Terms

For the purpose of these instructions

IT resources: devices, facilities and services that are used for electronic processing, storage, transmission or destruction of information such as computer systems, PDAs, data networks, software, internet access, e-mail, VoIP;

Users: all students and employees of the University of Lucerne as well as third parties who are authorised to use specific IT resources of the University of Lucerne (e.g. guests, congress members, affiliated organisations, library customers at public places of work);

PDAs (Personal Digital Assistants): personal microcomputers for managing dates and contact details as well as for communicating via mobile phone or data networks (wireless) by means of e-mail, voice, or video and for accessing internet content;

Boundary data: data used for the technical transmission of messages (e.g. addressing data at the head of electronic messages and information for session creation in accordance with technical communication protocol);

VoIP (Voice over IP): phone service via data networks, specifically IP networks.

Frohburgstrasse 3 · Postfach 4466 · 6002 Luzern
T +41 (0)41 229 50 10
helpdesk@unilu.ch
www.unilu.ch

1.3 Scope

These instructions apply to every use and joint use of University of Lucerne IT resources and also of IT resources not belonging to the university that are operated in the University of Lucerne data network.

2 Section II: Use

2.1 IT resources for employees

In principle employees of the University of Lucerne with a workload of at least 50% at the start of their employment are provided with a personal computer. Temporary lecturers are excepted from this.

For reasons of security and efficient use of energy the personal computers are to be shut down and switched off at the end of work.

2.2 Use of private IT resources

Private IT equipment (laptops, PDA, etc.) may only be connected to the University of Lucerne data network in accordance with the guidelines of the IT services and in particular only to networks specifically intended for this without access to internet servers or internal workstation computers.

Installing private software onto University of Lucerne equipment is strictly prohibited. Exceptions require authorisation from the IT Services.

2.3 Private use of University of Lucerne IT resources

The use of the IT resources is strictly for performing university tasks in accordance with the university legislation.

Private use of the IT resources is permitted where the use

- infringes neither these instructions nor the law nor the rights of third parties,
- is not of a commercial nature,
- does not involve bulk sending of e-mails,
- does not hinder work or study obligations,
- does not cause technical malfunctions,
- does not place disproportionately heavy demands on widely used IT resources (networks, internet access, etc.). In particular the use of peer-to-peer software (P2P), the user of internet radio and TV as well as downloading very large files such as music files, films, disk images, etc. is not permitted.

Storing private data on the University of Lucerne's servers is not allowed.

2.4. Access authorisations

The access authorisations for University of Lucerne IT resources that are operated by the IT Services are laid down by the IT Services.

Access-protected University of Lucerne IT resources are only accessible after successful authentication by means of a personal access authorisation means (password, PIN, chip card, token, etc.).

The access authorisation means are allocated to the users by the IT Services.

The access authorisation means are to be treated absolutely confidentially. Disclosure of or giving access to personal access authorisation means to third parties is prohibited.

The IT Services issue minimum requirements regarding the security of passwords and other access authorisation means.

If the suspicion arises that an access authorisation means has been disclosed or made accessible to unauthorised persons or has been used by them, the user must report this to the IT Services immediately.

2.5 Data privacy

Processing personal data is only allowed within the scope of the statutory purposes of the University of Lucerne as well as in accordance with the data privacy provisions.

For employees of the university the law on the protection of personal data (Data Privacy Act) of the Canton of Lucerne applies in particular.

2.6 Abuse of IT resources

Abuse is any use of the IT resources that

a) violates these instructions,
b) violates other provisions of the law,
c) infringes third party rights.

The following actions are in particular considered as abuse:

- Processing, saving or transmitting material with illegal or indecent content such as e.g. representations of violence, pornography (Art. 197 Swiss Penal Code), incitement to criminal acts or violence (Art. 259 Swiss Penal Code), attack on the freedom of faith and culture (Art. 261 Swiss Penal Code) or racial discrimination (Art. 261bis Swiss Penal Code). Exceptions for the purpose of teaching and research may be admissible but require approval by the rector;

- The creation, instruction for creating or deliberate distribution of harmful programs or program parts as referred to in Art. 144bis (2) Swiss Penal Code (viruses, worms, Trojans, etc.);

- The unauthorised hacking into a data processing system (Art. 143bis Swiss Penal Code ("hacking"): spying on passwords, unauthorised searching of internal and external networks for weak points (e.g. port scanning), providing and carrying out measures for disrupting networks and computers (e.g. denial of service attacks). The use of port scanners, sniffers, network analysis devices, etc. by the IT Services for performing their tasks is allowed;

- Data theft (Art, 143 Swiss Penal Code) and data corruption (Art. 144bis (1) Swiss Penal Code);

- The use of University of Lucerne IT resources in deliberate infringement of licence provisions or copyrights (e.g. illegal copying of data and software of any kind);

- Sending messages by electronic means of communication with fake or misleading sender details (including technical address) or of unsolicited advertising e-mails (spam);
- Harassing or misleading members of the University of Lucerne or third parties by messages with electronic means of communication (e.g. with insulting, sexist, racist, defamatory or discriminating content);
- Setting up direct connections to the University of Lucerne data network (e.g. by installing WLAN access points or modems)

2.7 Consequences of abuses

If an abuse is determined or if concrete suspicion of an abuse of IT resources is present, the IT Services can take the following actions:

- Provisional blocking of access to the IT resources affected by it,

and, after consultation with the rector, Human Resources or Data Protection Officer of the canton of Lucerne,

- Blocking improper and illegal data as well as securing and storing it for evidence purposes,
- Deleting improper and illegal data where this is necessary for reasons of security.

By order of the rector further actions can be taken:

- As sanctions against abuse, guilty users can be faced with blocking of the access to IT resources, with restriction of use or prohibition of use.
- In addition disciplinary actions can be taken against guilty users, civil proceedings (claim for damages) can be initiated or criminal charges pressed.
- Particularly serious cases may lead to expulsion or dismissal.
- The University of Lucerne may pass on the costs caused by abuses and their consequences, including clarification and sanctioning, (investigation, court and solicitors' costs) to guilty users.

3 Section III: Monitoring

3.1 Monitoring and surveillance measures

Monitoring and surveillance measures are in the first instance for checking and ensuring the technical security, the functionality and availability of the IT resources.

Records on the use of the IT resources are admissible for boundary data, in particular regarding the use of the University of Lucerne's servers and the incoming and outgoing data traffic, as well as for checking the observance of licence terms.

Only the employees of the IT Services may have access to the protocol data.

The content of e-mails, other electronic messages and other documents stored by users on personal devices or in personal areas on servers must not be read without the consent of the users affected.

For security reasons, to prevent abuse or to limit individually excessive data traffic, access to certain internet addresses can be limited or prevented by means of filter blocks.

If there is concrete suspicion of abuse, the IT Services may after written notification carry out corresponding checks (if personal rights of users are affected only after consultation with the rector, Human Resources or Data Protection Officer of the Canton of Lucerne).

The IT Services may in addition for reasons of system and data security carry out operational security controls at the workplace devices of the employees.

Employees of the central services of the University of Lucerne are empowered to check the authorisation of users for working at public work stations by means of ID checks (in particular of the student ID).

4 Section IV: Responsibility and Liability

4.1 Personal responsibility

Every user is personally responsible for ensuring that his use of the IT resources does not violate provisions of these instructions or the law (criminal law, data protection) or infringe third party rights (e.g. copyrights, licence provisions, personal rights).

If a user uses third party services subject to charge without the written consent of the superior or lecturer responsible, he must bear all associated costs himself.

External data media such as CDs, DVDs, floppy disks and USB sticks are to be checked for viruses before use.

4.2 Liability

Users must use the IT resources made available to them by the University of Lucerne with the required care. In the event of damage and technical malfunctions caused grossly negligently or deliberately to the University of Lucerne IT resources the person causing them is liable in every case. The improper use or violation of the instructions is considered as grossly negligent.

In the event of grossly negligent or deliberate infringement of third party rights (in particular copyrights and licence provisions) the user also becomes liable for any damages that may be claimed from the University of Lucerne by third parties.

The University of Lucerne assumes no liability for defects in IT resources and their consequences.

The present instructions come into force as of 1st June 2010.

Lucerne, 1st June 2010