Marina Dividian {revision 4} 25.01.2011

Universitetet i Stavanger

IT regulations for the University of Stavanger

Content

These regulations apply to the use of the university's IT services. The IT services comprise public computers and IT systems, networks, applications, data, etc. made available by the university, including local, national and international networks or other machines and systems that are accessed through such resources. The regulations apply to employees, students and others who are given access to IT services, called users.

These regulations shall be posted in appropriate locations such. computer rooms and be made available in electronic form. It can be obtained by contacting your local IT department. The regulations will also be handed out at first time user registration, or otherwise be made known to users.

A user is required to stay informed about current regulations and any supplementary provisions. Such provisions must be approved by the IT board.

Violation of the rules concerning privacy, confidentiality etc. can lead to liability and / or punishment. The standard rules regarding dismissal of workers or disciplinary measures against students may apply to users of IT services.

1. Safeguarding of rights

- Users agree to respect the rights of others, and are therefore dependent on agreement with the licensee. This applies both to software and other copyrighted information as text, picture and sound.
- Users are responsible for the use of information, programs, etc. made available through IT Services.
- Users are not permitted to copy programs and data using university equipment beyond what is required by the license agreements that the University has entered into
- University disclaims liability for economic loss caused by errors or omissions in applications, data, use of information from available databases or other information obtained through the network, etc.

Approved by: _____

2. User responsibilities

IT resources at the University of Stavanger are a tool to support the daily work, teaching, research and studies. This includes computers, printers, networks, internet and software. Resources are limited and everybody has a responsibility to ensure that equipment is used effectively for the tasks it is intended. Many of the resources are interconnected via the network, locally and nationally, and can be used for communication and information gathering. In this context, one must behave according to basic ethical standards, similar to the rules for the general good behavior in other relationships in society.

At the University of Stavanger users of IT services are expected to follow certain rules:

- The University has rules for the use of IT services to be followed by staff and students.
- In certain situations it is possible for master and doctoral students at the university to link their own computers to the university network. All other equipment not purchased through the IT department may not be linked to school networks.
- Students should always be able to identify themselves with student ID cards while using the computer equipment.
- When a user logs into the IT services s/he must always identify him/herself by user name, password or in other regular manner.
- Users have a duty to follow the IT staff's instructions for the use of IT services. They also have a duty to familiarize themselves with the software, documentation, etc. in a proper manner so that the possibility that ignorance may cause any malfunction or loss of data, programs or equipment can be reduced.
- Upon termination of employment, study or use the user is responsible for ensuring that copies of data, programs, etc. owned / managed by the university can be secured by the IT department. Other files, stored under the user's name, must be deleted by the user. If this is not done within a reasonable time, and at the latest within 3 months, the IT department can delete such files.

Approved by: _____

3. The use of private IT equipment at the university

Master and PhD students have the opportunity to link to the university's computer networks provided that the relevant rules are observed:

- The IT department is not responsible for this equipment. Any damage or loss arising from the use or misuse of this equipment is the responsibility of its owner. The IT department cannot be expected to provide equipment to make it possible to link up to LAN. Before equipment is placed in the university premises, the following must be clarified with the IT department:
    - who is the owner (s) of the device
    - who has operational responsibility for the unit (one person)
    - who has access to use the device or its network address and the physical location of the IT equipment
- The equipment and any software should be configured as specified by the IT operational staff.
- The equipment must not be used by persons other than those already registered as users of the university computer equipment. This means that no users will be registered for Unix machines or other multi-user machines who are not employed or studying at the university or have any other connection to the university.
- Server functions, information bases etc., e.g. ftp- or www servers that will be available from equipment outside the school's local network via external communication channels, should not be used without specific and explicit permission from operations staff in the IT department.
- The equipment must not be used for unauthorized storage or distribution of software. This also applies to legal software as freeware and shareware.

4. Computer Security

- Users at the University will be registered as users of the computer system and assigned a username and a password. It is the user's obligation to protect username and password to prevent unauthorized use. It is not permitted to gain unauthorized access to computer resources by using other usernames than one's own.
- It is not permitted to gain access to other users' data, software and storage areas without explicit permission from the other user.
- A user must not contribute to disrupting any part of the system or otherwise cause harm to others.
- It is not allowed to use anonymity, pseudonyms or false identity on the network. This also applies to all services on the Internet.
- Backups of all data on the central servers are made daily. For, The user is responsible for backup of data on other storage devices.

Approved by: _____

- Computers must not be modified without the explicit permission of the IT department. It is not allowed to disassemble equipment to remove parts, add parts, change the hardware and / or software configurations, or remove equipment from the place where it is located. Everybody must be observant and help to ensure the university against theft by following the rules for access to buildings and equipment.
- Users are not allowed to set up or use their own IT equipment at the university unless this has been cleared with the IT department (see application form).
- It is not allowed to set up separate information servers (www, ftp, irc, etc.) or multi-user systems (Linux, Unix, NT server, etc.) without prior agreement with the IT department (see application form).
- The University reserves the right to supervise, inspect, alter or remove any file or system resource that undermines the authorized use of computer equipment.
- Attempts to prevent system administrators' access to system resources is considered unauthorized use.
- The University disclaims liability for any losses incurred as a result of efforts to preserve the system integrity of the data network.

5. Privacy Policy

- A user must not attempt to gain unauthorized access to other persons' computer, applications, passwords or other security elements.
- A user is required to be familiar with the rules that apply to personal information in particular. Computer-based files containing information about individuals or about companies or organizations (natural and legal persons) can normally only be created with the consent of the Data Inspectorate.
- If a user wishes to register personal information, s/he must ensure that this is permitted by the person registry law or regulations issued pursuant to the Act, or pursuant to a license granted to the university. If the register is not to be accepted according to the above rules, the user must apply for the necessary permission. The person responsible for the operation will provide advice on how users should proceed.

6. UiS-IT's right to access users' reserved areas

The IT department has the right to access the individual user's reserved areas in the facility in order to:

- Ensure the proper functioning
- Verify that the user does not violate or have violated the provisions of these regulations. It is assumed that such access will only be sought when it is of great importance for the operation or the university's responsibility, and only on special grounds for suspicion. Permission for access to electronic mail must be applied for separately. The IT department does not have access to a user's restricted areas without special permission from the IT Director, Resource Director or the University Director.

If the IT department seeks such access prior permission must be obtained from the University Director, unless there are particularly compelling reasons for immediate action. Such weighty reasons must be documented to the University Director after the action.

If the use of a workstation, terminal or other end user equipment is monitored by the IT department due to maintenance or other concerns, it must be clearly marked with a label or other appropriate means.

The IT department has a duty to maintain confidentiality regarding information about the user activities that can be obtained in this way, with the exception of acts, that may constitute violations of the regulations, may be reported to superiors.

7. Sanctions for violations of regulations

- Violation of these rules may lead to shutdown of the user's access to the university's computer system completely or partially. To determine whether a violation has occurred the administrator can block a user's access from up to 5 working days.
- Violation of the regulations from particular parts of the computer system may lead to shutdown between this section and other university networks wholly or partly. To determine whether a violation has occurred and to ensure against new violations, the administrator can shut down the connection completely for up to 5 working days. The Resource Director, or a person acting on behalf of the University Director, will determine whether the connection to the university's other networks will be closed completely or partially.
- Violations of these regulations shall be reported to the user's faculty or unit that will determine whether the user's access to the university's computer system should be shut down completely or partially. Their faculty or unit should also consider whether the offense leads to disciplinary action.

Approved by: _____

8. Information servers at the university

- For the purpose of education it may be convenient for employees, students or groups at UiS to be granted permission to operate an information server connected to the network. This can be done upon agreement with the IT department and provided that the following rules are observed.

- The IT department and the university carries no responsibility for the software and the information disseminated. Any damage or loss arising from the use or misuse shall be borne by the person responsible for running the server.

- The IT department cannot be expected to make equipment and software available to link the server to the LAN. Before the information server is established in the university premises, the following must be clarified with the operation staff in the IT department:

    - Who has the operational responsibility for the server (a person).
    - What kind of information will be stored.
    - The physical location of the server.
    - The server must be configured as assigned by the operating personnel in the IT department.
    - The server must not under any circumstances be used for storage and distribution of software and information that is not legally and publicly available.

- The person responsible for the operation of the server is also responsible for ensuring that these rules are followed:

    - The server must at any time be accessible for operating personnel in the IT department.
    - The IT department can, when necessary, without notice disconnect the server from the network at any time.
    - The permission is time-limited and granted only for the current semester, i.e. up to June 31 or December 31.

Approved by: _____

9. Netiquette (Good manners online)

- The user has a shared responsibility for IT resource utilization. This means the time and capacity for both computers, networks and personnel related to the IT services.
- A user must be very cautious with the use of IT services for activities not directly related to academic activities, administration, research, study or organizational work in connection with the university.
- IT services must not be used for commercial purposes or for activities unrelated to the activity that takes place at the university.
- Users shall not use IT services to make defamatory or discriminatory statements, illegal downloading of music / movies / pornography, or to disseminate confidential information, violate privacy or encourage or participate in illegal or irregular actions.
- Use of computer equipment and software that involves the use of resources outside the university shall be limited and not be used for personal entertainment. Access to international public data resources is a privilege, and the users at the university are required to prove worthy of trust.

Any use of IT services must be made in accordance with Norwegian law.

IT-regulations