RULES

2005-08-01

1 Principles

Computing facilities, networks, peripheral equipment and accounts are owned and operated by the University of Skövde for use in work authorised by the University.

The University cannot be held responsible for any problem due to disturbances in the function and availability of the systems.

The University reserves the right to impose restrictions concerning publication and distribution of material via the equipment of the University.

An *authorised user* according to these rules is a person who is assigned an account or any other person who has permission to use computing facilities, networks or system resources belonging to the University.

An authorised user is committed to the following rules:

- Authorisation and accompanying resources can only be used by an authorised user and solely by the person to whom authorisation was granted.
- The password accompanying the authorisation must be kept confidential.
- The authorisation is time-limited and expires at the end of studies, employment, a project (or corresponding stay at the University).
- The University reserves the right to terminate an authorisation that has been inactive for more than six months unless otherwise agreed.

According to a special decision by the chancellor the authorised user must sign a user agreement. This can be done either by signing the user agreement, or by electronic verification.

2 Rules for Using Computers

In addition to existing law the following rules apply.

2.1 General Rules

Sabotage or other disruptions to the system or to other users and also infringement or attempts of infringement to local systems as well as systems outside of the University are strictly forbidden. Consequently it is forbidden to modify, delete or in any other way influence system files and other files that are necessary in order for the system to function. Furthermore, it is also forbidden to delete, read, modify or write any file without the authorised permission by the owner of the file.

Commercial use of the University's computer resources is strictly forbidden. The University has to make sure that all users are committed to existing license agreements. Consequently it is strictly forbidden – unless stated otherwise – to copy software installed on the University computer systems and install them on other computers (e.g. own computers). Furthermore, it is strictly forbidden to use available resources (including the network) for commercial purposes.

Users must login via the username assigned by a system administrator. Using other accounts is strictly forbidden. The user must ensure that the password is "secure". An instructor or system administrator can provide information regarding the selection of a safe password (see section 4 below).

Users who detect any errors, security problems, violation of rules, improprieties or any other problems must immediately notify this to the responsible system administrator.

It is strictly forbidden to store and install programs without permission from the responsible system administrator.

Storage of files is only permitted in the user's home directory and in space specially designated for the purpose intended.

The system administrator may, without notice, delete files considered interfering with the security, the integrity or the function of the system or in any other manner violating of existing rules.

The person responsible for data protection is, within his field of responsibility, entitled to examine the contents of traffic, data etc. that is stored or under transmission, in order to check that these rules are complied with.

Special rules for employees

Usage of the University computer resources for activities other than what the University has decided, such as own development, is only permissible when

- regular use is not disturbed
- it does not involve a violation of these rules or signed agreement
- it does not conflict with the rules of the working group, the rules and the guiding principles of the University in general and the rules of SUNET (Swedish University Network).

Special rules for students

The University's computers in computer rooms and lab rooms may only be used for research and education purposes in compulsory work that is part of the examination of a course (education), individual skill training as a complement to theoretical and practical studies related to knowledge obtained during the course.

A student can only use the computer resources of a department during the time the student is enrolled in a course offered by the department.

3 Ethical Rules

The University is connected to SUNET and its rules for using computer networks. The rules state the following:

It is a generally accepted principle in the academic world that the networks be kept as open as possible. In order for this to happen it is unavoidable that certain ethical requirements are placed on the individuals who use the networks and on their activities. These ethical requirements do not differ markedly from other requirements placed on citizens in a modern society.

SUNET condemns as unethical any attempts

- to gain access to network resources without having the right to do so
- to hide his/her user identity
- to disturb or interrupt legitimate use of the networks
- obiously wastes available resources (staff, hardware, software)
- to damage or destroy database information
- to insult or humiliate other users

In addition to SUNET's ethical rules, the user is required when using computer resources to act in such a manner as not to cause the University or others unnecessary costs or a bad reputation. In the case of electronic publication the legally responsible person must always be indicated (this person is personally responsible for the contents).

4 Password

Users must observe the following when choosing a password:

- The password must be eight characters long
-Words occurring in any dictionary or a combination of such words and numbers must not be used
- Telephone numbers or personal numbers, names of friends, pets etc. must not be used

- Passwords must be easy to remember
- The password must contain one number, one lower letter and one upper letter
- The password must not include any specific Swedish characters (i.e. å, ä or ö)

The instructor or responsible system administrator must be contacted if there are any problems or doubts.

5 General Safety Rules and Regulations for Students

The following rules apply for all computer rooms:

-No form of food or drink must be consumed
- At the end of each working period the workplace must be restored to the condition it was in the beginning of the working period (or better).
- If a student leaves a terminal or computer for more than 20 minutes, he/she must log out.

The last person leaving a computer room is responsible for closing the windows, turning off the lights and locking the door, this is in order to prevent unlocked and unmanned computer rooms. Lock codes and/or similar keys must not be passed on to other persons. The person who opens a room has to make sure that no unauthorised person is admitted. The use of computer rooms without supervision requires trust and responsibility.

Orderliness is important during computer use, therefore it is not suitable to put clothes, bags, etc on computer tables. Furthermore, heavy bags and jackets may damage sensitive equipment.

6 Consequences of Breach of Rules

The person responsible for computer security must notify any violation of these rules, agreements and existing laws to the appropriate division manager. A serious violation of rules is reported to the police after a decision by the chancellor. Serious violations could result in legal consequences and may involve fine or criminal prosecution. In some cases breaches may be reported to the Disciplinary Board.

In all other cases, it is the appropriate division manager who decides on further actions, for example, suspension of the user’s account while awaiting further investigation.

The person responsible for computer security and the person responsible for system administration are bound by professional secrecy. This secrecy does not, however, apply to situations where a crime may have been committed.

The person responsible for computer security is, under ongoing investigation, authorised to suspend access to the University’s computers, network and system resources in cases of well-grounded suspicion of violations of rules, agreements and existing laws.

7 Information

Existing rules must be available on the web.