Rector's Directive No. 13/2011

Rules of use of the Silesian University computer network

I.

Subject matter, definition of basic terms

1. This Directive defines binding rules for the use of the computer network of the Silesian University (hereinafter referred to as "SU"). It applies to all users of the SU computer network (employees, students, or third parties) and all computers or similar devices that are directly connected to the computer network or its computers by any means.
2. Computer network (or just "network") means all technical and software resources of computer systems of individual SU units and their departments (university-wide departments, faculties, departments, institutes, etc.) and all means for interconnecting these systems.
3. A computer network user is anyone who directly uses a computer network, computers or other devices connected to it.
4. The administrator of a network (or part of it), server or computer room (laboratory) is the SU department that manages the network, server or computer room (laboratory).
5. An administrator is a person who is authorised by the administrator of a particular computing system to perform activities related to the system administration and maintenance of the entrusted system.
6. Computing resources means the aforementioned computers or network.
7. A computer virus is any executable code or macro code that is installed on a computer without the knowledge of the user or computer administrator and whose primary purpose is unauthorized activities by the user, including but not limited to modifying data and programs on the computer, collecting information about the computer and files stored on the computer, sending itself and/or data from the computer to other systems, and sending incorrect data over the network.

II.

General provisions

1. The SU network is a distributed network with a certain degree of hierarchy. The network consists of individual domains (subnetworks) that are created according to the individual SU components and their locations. The SU network is connected into larger units – the Czech academic network CESNET and the global Internet network – and is built in accordance with the principles of building these networks.
2. The individual domains are managed by the parts of the SU that created them, in close cooperation with each other. The specific administration is carried out by the staff of the relevant departments of the individual SU units or by officially authorised staff of individual departments or institutes (hereinafter referred to as "administrators").
3. The network administrator in each domain is the administrator of the computing resources in that domain. They ensure that their operation does not restrict or even damage the operation of the university-wide network. Changes to the configuration of the network within their domain are entirely within their competence.
4. The network administrator is authorized to monitor the activities of users of the managed domain within limits that do not jeopardize the public, personal or proprietary rights of individual users. They are obliged to keep the information with which they come into contact in the course of this activity absolutely confidential and are not entitled to make the contents of the private directories of individual users known to other persons. In the event of a detected violation of the rules of operation of the SU network, they are obliged to inform the responsible manager of the relevant SU unit of this fact. As part of monitoring, the network administrator may also monitor users of subdomains that fall under their domain.
5. The network administrator may disconnect a subdomain to which technical resources have been connected that have not been consulted or on which a network software configuration change has been made that has not been consulted, and those resources or that change have led or could lead to a serious malfunction that threatens the operation of the university-wide network.
6. The network administrator is authorized to establish additional binding rules in the managed domain, regulating specific activities necessary for connecting computer systems (recommended operating system including mandatory updates, name server specifications, communication protocols, degree of openness of some network services, etc.).
7. The administrator of a particular computer in the network, not the network administrator, is responsible for assigning user accounts and other resources to that computer.
8. The user is responsible for backing up their data. The user shall consult the appropriate network administrator on the method of backup.

III.

Property rights

1. Users use the SU computer resources in accordance with their work and study tasks. Effective fulfilment of these tasks requires mutual cooperation of users while strictly respecting the property rights to data stored in electronic form. When accessing this form of data storage, users must follow exactly the same ethical and legal standards as when accessing objects and information in other forms.

2. All components of the SU computer network are property of the SU, or the SU owns or exercises usage rights to them. The inadmissibility of theft or damage then applies to the electronic form of data and information as well as to the physical assets themselves.

3. It is forbidden to SU employees, officials, and students in particular to:

   a. Connect additional computers to the network and move them without the approval of the network administrator.
   b. Install software that would disproportionately increase the load on the network and servers without the approval of network administrators.
   c. Distribute and install software and data to which the user does not have ownership or usage rights on the network.
   d. Copy even parts of software or data to which the user exercises ownership or usage rights in an unauthorised manner.
   e. Modify programs, data or technical equipment owned or used by the SU in an unauthorised manner. In particular, it is strictly forbidden to change the configurations of computers or other resources in an unauthorised manner which could affect the operation of the network as a whole.
   f. Damage or destroy computer resources (computers, software or communication lines).
   g. Exploit the negligence of other users (e.g. failure to log out, inadequate file protection) to access someone else's identity or data.
   h. Use software in a way that may lead to the acquisition of someone else's identity and use of software to obtain unjustified anonymity (e.g. sending anonymous mail, etc.)
   i. Attempt to obtain access rights that have not been granted by the administrator (e.g., unauthorized access to any non-public information resources both at SU and in any organization accessible via the computer network). If the user obtains such rights due to a software or hardware error, they are obliged to immediately notify the administrator of this fact.
   j. Eavesdrop or otherwise monitor network traffic and make copies of messages passing through individual nodes in the network. If such activity is to be carried out in the context of teaching of specialised subjects by a specialist department (institute), it must be carried out exclusively in the laboratories of that department (institute) under conditions to be determined by the network administrator of that laboratory.
   k. Use SU computer resources for activities listed in a) to j) above against any other organisation whose computer resources are accessible via the SU computer network.

IV.

Data and information protection

1. SU strives to protect the civil, personal, and property rights of all users of the computer network and, in this context, to protect the privacy of data and information stored on SU computers and/or transmitted over the computer network.

2. To ensure the maximum possible level of data privacy and security, users are prohibited from:

   a. Taking any action that results in a breach of another user's privacy, even if that other user is not explicitly protecting their own data.
   b. Copying any data or programs from user directories without the permission of their owners. This restriction applies even if the user directories are left freely accessible by

electronic means by their owners.

c. Knowingly using illegal software and data or offering such software or data to others.

d. Using the network for the dissemination of commercial information, for advertising purposes, for political or religious agitation, and for the dissemination of material that is contrary to the law, general ethical and moral standards, or that may damage the name of SU. It is also prohibited to harass other users with mass messages, including chain messages or letters to randomly selected addresses on the network.

e. Using SU computer resources to commit crimes or administrative offences.

f. Using the computer network to gain unauthorised access to non-public information resources (including those owned/managed by others).

V.

Protection against computer viruses

1. Several levels of protection against the threat of computer viruses are in place at SU. Its first and basic part is the virus protection of individual computers, ensured by the installation of a suitable antivirus program and its correct use on all computers. Another level of protection against computer viruses is the checking of incoming and outgoing mail at SU.
2. Each user is obliged to monitor the information provided by anti-virus programs and in the event of detection of a virus infection they are obliged to prevent the further spread of the virus (usually by shutting down the computer), inform the network administrator about this fact and cooperate in providing remediation.
3. Every electronic letter whose addressee is from the SU (slu.cz) domain is verified by the anti-virus program and, if a virus is detected, marked accordingly. Further handling of a letter with a detected virus is subject to the rules defined by the SU components. These rules must provide sufficient protection against automatic or unwitting activation of the virus by the final recipient.
4. Every electronic letter that is sent from SU is also checked for the presence of a virus. A letter containing a virus is deleted and a warning is sent to the sender.

VI.

Access rights and user identification

1. Access to a computer network requires that each user can be uniquely identified.
2. Every SU employee and every SU student has the right to set up a user account (hereinafter referred to as an account) on a suitable network computer. The suitability of the computer must be understood both in relation to the SU unit/workplace and the purpose for which the user is requesting the account; users may generally have multiple accounts on the network. Appropriate access rights are associated with each individual account and these determine the user's privileges in relation to network resources.
3. SU employees shall be granted access to the network's computer resources on the basis of a request made by the head of a department to the relevant network administrator. The head of department is also required to notify the administrator of the termination of the employee's employment at the department so that the employee's account can be terminated. Staff access

rights to specialised servers (SU information systems, etc.) shall be allocated by the administrators of these servers on the basis of precise requests from the relevant heads of staff.

4. SU students acquire access rights to the SU network on the day of enrolment for studies at SU.
5. The creation of user accounts on servers managed by individual departments is the responsibility of those departments.
6. The user for whom the account is set up is obliged to secure the account with a non-trivial password and to keep this password secret.
7. The user must not disclose the password to their own (individual) account to another person (even to the administrator of the computer on which the account is set up).
8. The user may only use access rights that properly belong to SU and may not take any action to circumvent this provision. If the user in any way acquires access rights that have not been assigned to the SU (e.g. by a software or hardware error), they shall immediately notify the computer administrator of this fact. They may not use the rights thusly obtained.
9. A user may make their account available to other users of the computer network, subject to the following conditions:
   a. Access is only available to a person who has an individual account registered in the SU network, or is a student or employee of the SU, or is in a valid contractual relationship with the SU, the content of which includes access to the SU computer network.
   b. Access is not made by communicating the password, but by other means allowed by the operating system in use. In this case, however, the user is jointly responsible for any misuse of the account for activities contrary to these rules.
10. A user must not take advantage of another user's negligence (e.g., failure to log out) to work on the network under someone else's identity.

VII.

General obligations

1. When communicating with other networks, the user is obliged to follow the rules that apply in these networks.
2. The user shall strive to ensure that their activities have minimal negative impact on the use of computer resources by other users. This applies both to disproportionate burdening of lines at times of maximum use and to disproportionate burdening of individual computers. It is advisable to consult with the computer/network administrator for all such activities and to follow their instructions.
3. The use of the SU network for scientific and pedagogical cooperation by students and employees of other organisations is possible on the basis of written permission issued by the head of the relevant unit or the Rector. In the case of a relationship lasting longer than an academic year, it is necessary to specify the specific conditions of use of the SU computer network, including possible sanctions, in the contract between the SU (a specific unit) and the organisation whose employees use the SU network. This contract does not have to be concluded in the case of cooperation with employees or students of other universities or institutes of the Academy of Sciences.
4. The use of the SU network for purposes not directly related to the mission of the SU is possible only on the basis of written permission issued by the Rector of the SU.

VIII.

Sanctions

1. The network administrator shall have the right to temporarily or permanently restrict or withdraw user access rights to the computer network from users who are proven to have violated the provisions of this Directive. The user has the right to ask the head of the relevant unit or, in the case of units with a university-wide scope, the Rector of SU to reconsider this measure.
2. Violation of the provisions of this Directive by a student shall be considered a disciplinary offence within the meaning of §64 of Act No.111/1998 Coll., on Universities and on Amendments and Supplements to Some Other Acts (Act on Universities), for which a sanction may be imposed in accordance with the above-mentioned Act and the SU Disciplinary Regulations pursuant to §65 (1) of Act No.111/1998 Coll.
3. Violation of the provisions of this Directive by employees will be considered a violation of the employee's basic duties (Section 301(c) and (d) of the Labour Code) and may result in appropriate employment consequences, including termination of employment.
4. Violation of the rules of virus protection, especially arbitrary disabling of this protection with subsequent infection of the computer or computers of the SU network will always be considered a serious breach of work discipline.

IX.

Final provisions

1. This Directive shall become effective on the date of its issue.
2. This Directive cancels Rector's Directive No. 17/2004.
3. I delegate the control of compliance with these rules and their further interpretation to the relevant administrators of the SU network.
4. Each network administrator shall have the right to issue internal guidelines and regulations to tighten, specify or clarify the provisions of this Directive applicable to a particular workplace.

Opava, 13 September 2011

Prof. PhDr. Rudolf Žáček, Dr.
Rector