University of Chemistry and Technology, Prague

Title	**INTERNAL STANDARD No. A/N/961/1/2018**
Subject	**Rules for the use of computers and computer network at the University of Chemistry and Technology, Prague**
Applicability	All school
Effective from	March 1, 2018
Effective to	Indefinite term
Issued by	Karel Melzoch

Article 1

Applicability and purpose

(1) These rules for the use of computers and computer network at the University of Chemistry and Technology Prague (hereinafter the "rules") govern the binding procedure for using computers and other devices (hereinafter "computer devices") that are directly or remotely connected to the computer network of the University of Chemistry and Technology Prague (hereinafter "UCT").

(2) These Rules apply to the use of any computer devices owned by natural or legal entities (hereinafter the "User") and running in or accessing remotely the UCT computer network. The purpose of the rules is to protect UCT against abuse and unauthorised use of computer devices and the UCT computer network as well as the data stored in the network.

Article 2

Definitions

(1) For the purpose of these Rules the following expressions shall have the following meanings:

a) Computer devices – namely computers, mobile computer devices, printers, measuring devices and other electronic devices that may be connected to the UCT computer network;

b) UCT computer network – sum of hardware and software means in all UCT premises necessary for interconnecting the devices and users;

c) User of computer devices – any person using any of the devices stated in letter a) or the UCT network;

d) Legal software – computer programme acquired in compliance with generally binding legal regulations, namely in compliance with the Copyright Act;

e) UCT computer network administrator – Computer Centre of UCT (hereinafter the "Computer Centre"). The Computer Centre is responsible for the security of the UCT computer network;

f) Administrator – authorized employee of the Computer Centre;

g) User identification – user authentication and subsequent authorization. Authentication and authorization are security measures that serve for unambiguous identification of a user who accesses the system. It is a unique method of identification of an employee, student, other user or device meeting the conditions for internal identification of a person, including electronic signature or electronic verification of documents not requiring verification under Act No. 297/2016 Coll., on trust creating services for electronic transactions. User identification serves also for setting up access rights to UCT information systems;

h) Authentication – verification of authenticity and correctness of unique credentials of the user, namely by combination of user login and password, or with the help of electronic signature, authentication token or biometric data;

i) Authorization – the process of verification of access rights of a user entering the information systems in order to perform certain activities;

j) Person responsible for computer hardware of the workplace (hereinafter "person responsible for hardware") – person appointed by the head of the workplace and responsible for the administration of the hardware at the workplace provided that this responsibility is not the task of the Computer Centre in cooperation with the person who ensures communication of the users of the workplace with the administrator.

Article 3

Authorized users of computer devices

(1) Computer devices or computer network within UCT may be used by the following authorized users:

a) academic and research staff of UCT,

b) other employees of UCT who need the devices for their work,

c) other persons upon agreement with the head of the workplace, with the person responsible for computer hardware, with the administrator or the vice-rector responsible for the work of the Computer Centre, depending on the nature of the work on the specific device within the UCT network – for the use of computer devices at a workplace it is the person responsible for computer hardware or the head of the workplace who are the responsible person, for all other devices it is the Head of the Computer Centre, and for providing access to information database systems it is the Registrar of UCT,

d) UCT students within the lessons, preparation for lessons or scientific, research and other creative activities provided they are not subject to limitation under other provisions of the Rules,

e) till the day of enrolment to study in master or doctoral study programme (Study and Examination Rules of the UCT Prague, Article 2, paragraph 1), all students who have duly completed their study (bachelor or master) and have applied for the follow-up type of study (master or doctoral) or who have been granted an exception by the responsible employees of the Dean´s Office of the respective faculty.

(2) Authorized user is obliged to verify, by appropriate technical means, his or her authenticity and authorization, which may be e.g. user name and password, certificate, etc.

(3) Credentials of a user or of a device are unique and non-transferable to other users or devices.

Article 4

Access to computer devices and computer network

(1) Access both to the UCT network and outside the network is enabled only for scientific and research or pedagogical and study purposes and other support activities necessary in order to carry out work.

(2) User´s access (or access of a user group) to computer devices and computer network within UCT may be limited in case the computer devices are overloaded or modified in any way or abused by third party or if their operational status cannot be regulated by the Computer Centre or if allowing such device to remain in operation could cause intangible or other damage to UCT.

(3) By requesting to work in UCT computer network, each user of computer devices acknowledges monitoring of the activity of the device by employees of the Computer Centre.

(4) The purpose of the monitoring is to optimise the operation of the computer devices and the UCT computer network, to identify and prevent exceptions, and to detect cases of breach of the rules of using the network. The Computer Centre uses appropriate monitoring technical means for the purpose of ensuring security of the computer network.

(5) For the purpose of monitoring of the network operation, the UCT network administrator collects namely the following data: source and target IP address, name of device, verifying identity of user or device, source and target Ethernet address, port number (protocol number), date of transmission, duration of transmission and number of transmitted bites, type of the device´s operating system, list of software installed on the device. In addition, the UCT network administrator is entitled to run software on his or her servers in order to perform regular security audit. Security policy in the IT area is the responsibility of the Head of the Computer Centre.

(6) Computer devices with an operating system that are not supported by the manufacturer of such operating system and do not meet defined conditions for operation in the computer network, as well as computer devices with software containing publicly known (not corrected) vulnerability, are excluded from connecting to the UCT computer network.

(7) Access to the UCT computer network is not guaranteed to devices with hardware and controllers not supported by the manufacturer or whose support was terminated.

(8) The user is entitled to connect to the UCT computer network only such devices that comply with the technical and security requirements and the user is obliged to maintain the security of such devices at a level preventing unnecessary threat to other devices connected to the computer network.

(9) Connecting of device to the wireless UCT computer network is governed by a list of recommended protocols and technical standards which is published on the Computer Centre´s websites. The devices not supporting such protocols and technical standards will not have guaranteed access to the UCT computer network.

Article 5

Services provided to users

(1) The Computer Centre provides the following services to the users:

a) securing the computer network against leak, abuse of and damage to data as result of unauthorized access by an unauthorized person or intrusion of malicious software in the computer network,

b) backup of centrally administered data,

c) computer time on computers directly administered by the Computer Centre, including access to software purchased for general use at UCT,

d) electronic mail (e-mail) – each user has at least one unambiguous address (in the format Name.Surname@vscht.cz) and has the possibility to send and receive e-mails from local UCT network and the Internet,

e) helpdesk application, which serves to report and record user requirements,

f) access to servers and technical maintenance of information servers of UCT,

g) software and hardware administration of classrooms within the responsibility of the Computer Centre,

h) interactive access to Internet,

i) processing of UCT agendas,

j) programme support connected with operation and installation of software enabling access to and communication with UCT servers,

k) administration and innovation of computer networks at UCT,

l) setting up, closing and maintenance of user accounts.

(2) Due to security reasons, the provision of certain network services may be limited only to certain servers as decided by the UCT network administrator. Users are not given any guarantee of uninterrupted operation of the computer network, its availability or quality.

Article 6

User´s obligations

(1) The user undertakes not to disseminate and willingly use any software acquired contrary to legal regulations, namely the Copyright Act, and the user also undertakes that no software acquired in compliance with such regulations will be used by him or her in any manner contrary to the agreement by which the author of the software consents to the use thereof.

(2) An employee may use computer devices only within his or her job description, students within instruction and other agreed activities at the school´s workplaces. It is not allowed to use the network for commercial purposes.

(3) User access rights are given by user identification and membership in groups. Login name with the initial password are handed to the user on the commencement of his or her studies or employment at UCT. The initial password must be changed by the user at the first login and thereafter every 6 months at the latest. If the security situation in the network requires so, the password change may be enforced at any time. Password creation and its rules are described on the information website of the Computer Centre https://vc.vscht.cz/navody/zmena-hesla.

(4) By no means may the user try to gain access rights or a privileged status not assigned to him or her by the administrator of computer devices. If the user gains in any way (including hardware or software system error) a privileged status or access rights to which he or she is not eligible, the user is obliged to promptly report such fact to the administrator. The stated shall apply to all computers and computer networks to which the user gains access within UCT. The user shall not try to gain access to protected information and data of other users.

(5) The user is obliged, within his or her user rights, to safeguard his or her data to maximum extent against abuse by third parties.

(6) It is forbidden to copy or distribute even parts of the operating system and the installed applications and programs. Programs can be used only for such activity for which they have been designed.

(7) The user works on UCT computer devices only under the user name assigned to him or her. The user shall chose and keep confidential his or her password to the user name in order to avoid any potential

abuse. The user is responsible for any damage incurred as result of abuse of his or her account due to careless manipulation with the account.

(8) The same rules as for traditional mail shall apply to the use of electronic mail (e-mail). Namely it is forbidden to use e-mail for dissemination of commercial information, political or religious publicity and propagation of materials not compliant with legal regulations. It is also forbidden to bother other users by sending mass e-mails or by messages which by their nature are not related directly to the job position and duties.

(9) Official electronic communication between the user and UCT Prague concerning study and work matters is performed exclusively via unambiguous e-mail address in the vscht.cz domain assigned to each student and employee of UCT Prague.

(10) Major administration changes in the configuration of e-mail can be made only by the employees of the Computer Centre or in cooperation with them.

(11) The user communicates with the administrator via the responsible employee, except for cases stated in Article 6, paragraph 4 or other cases when there is danger in delay, either from the security point of view, or in terms of protecting the work of other authorized users.

(12) User websites must not be used for dissemination of information of commercial nature, political or religious publicity and materials not compliant with legal regulations or ethics.

(13) Authorized users of electronic information sources purchased by UCT or the National Technical Library are obliged to comply with the licence conditions valid for the individual sources and databases. The user is aware that the obtained information and data (in any form and on any media) serve exclusively for the user´s personal use and his or her study, pedagogical and research purposes. It is not allowed in any way to further disseminate, copy, lend, share, distribute (not even in computer network), sell or otherwise use them namely for commercial purposes. It is forbidden to create own copies of databases and to download entire years of journals or inadequate volumes of texts of electronic journals. The user is also obliged to respect intellectual property rights regarding data under Act No. 121/2000 Coll., on Copyright and Rights Related to Copyright and on Amendment to Certain Acts (Copyright Act) and other regulations.

(14) The user is obliged to keep his or her software updated on the device used to connect to the UCT computer network, to have an antivirus program installed in case of Microsoft Windows, to have firewall turned on and to follow other usual security rules.

(15) If it is necessary to connect a device with operating system not supported any more by the manufacturer, or a device on which antivirus cannot be run due to technical reasons, such device can be connected only upon consent of the responsible employee of the Computer Centre, who will define further conditions, if any, for the operation of such device.

(16) Computer devices that are used directly by the user for his or her activity are not backed up centrally. Users are advised to perform regular backups of their data. This provision shall apply only to employees and students of doctoral study programmes of UCT.

(17) The user works in the computer network in such way that does not interfere with the work of other users and does not prevent them from using the network devices.

(18) The user shall not intentionally overload the network. Should the user continue overloading the network in spite of repeated warnings by the administrator, the administrator will decide to use available technical tools to suspend the user´s access to the network.

Article 7

Obligations of the person responsible for computer hardware

(1) The person responsible for computer hardware shall make sure that the operation of the computer devices managed by him or her does not limit or interfere with network communication. Any changes in configuration that may affect the operation of the network shall always be agreed with the administrator.

(2) Except for standard computer devices acquired within purchases prepared and guaranteed by the Computer Centre, the person responsible for computer hardware performs physical connection of new devices to the network only in cooperation with the employees of the Computer Centre. Before such computer devices are purchased, the purchase has to be consulted with the employees of the Computer Centre in terms of network communication requirements.

Article 8

Breach of rules

(1) Any abuse of data and information acquired by using computers and the computer network at UCT is governed namely by the following acts:

- Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendments to Some Acts, as amended,
- Act No. 250/2016 Coll., on the Liability for Offences and Proceedings Related Thereto, as amended,
- Act. 40/2009 Coll., Criminal Code, as amended,
- Regulation 2016/679/EU GDPR.

(2) In case of any breach of these rules, sanctions may be applied under generally binding legal regulations and internal regulations of UCT. In compliance with general civil code and criminal code liability of the user under the respective provisions of generally binding legal regulations, UCT is entitled to compensation for damages incurred by the user´s breach of the obligations stated in this internal standard.

(3) In cases of breach of the stated rules or generally binding legal regulations by the user or in case of justified suspicion of abuse of user account or operating status of the device which threatens the security of other devices in the computer network or which limit the correct functioning of a devices administered by the Computer Centre, the Computer Centre is entitled to disconnect such device or user from UCT network. In urgent cases such as unauthorized modification of software by third party during attacks by virus, spyware, ransomware, etc., the user or device shall be disconnected immediately without unnecessary delay. The user shall be informed about such actions.

Article 9

Final provisions

(1) As at the date when this internal standard comes to force and effect, the Rules of Use of Computers and Computer Network at the Institute of Chemistry and Technology, Prague as of May 1, 2001, No. 20.10/01, shall cease to be effective.

(2) This internal standard was agreed by the Academic Senate of UCT Prague on the date of February 20, 2018.

Karel Melzoch

Rector