

Code:	SR/1/2016
Category:	RECTOR'S DIRECTIVE
Title:	Rules for Computer Network Use at TBU in Zlín
Liability:	Tomas Bata University in Zlín
Issue date:	1 January 2016
Effective from:	1 January 2016
Issued by:	Prof. Ing. Petr Sáha, CSc., Rector
Prepared by:	
In cooperation with:	
Pages:	5
Appendices:	
Distribution list:	Students and employees of TBU in Zlín
Signature of authorized person:	

Article 1

Basic provisions, definition of basic terms

- (1) Tomas Bata University in Zlín (hereinafter referred to as "TBU") runs a non-public computer network, which enables transfer of digital data for provision of the University's own electronic communication services, for TBU purposes, for management of TBU and for provision of access to internal and external digitized resources. This Directive sets out basic rules for use and operation of the TBU computer network.
- (2) The term "TBU computer network" (hereinafter referred to as "TBU network") refers to all technical and program tools serving for connection of computers and for use of this connection. The TBU network is distributed to all localities, campuses and buildings of TBU and is composed of several sub-networks. The TBU network is connected via CESNET2 (National E-Infrastructure for Science, Research and Education) to the Internet global network and built up in accordance with the rules for the building up of the networks mentioned.
- (3) A user of the TBU network (hereinafter referred to as "user") is every person that directly uses the above-mentioned TBU networks, computers and/or devices connected to them.
- (4) The term "user account" (hereinafter referred to as "account") involves the authorization to use a particular computer; each user has a unique user identification. Usually, it is a user name and a password.
- (5) The TBU Information Technology Centre (hereinafter referred to as "ITC") is the global administrator of the TBU network.
- (6) The administrator of the TBU network (hereinafter referred to as "TBU network administrator") refers to the person/persons in charge of administration of all tools and devices in the TBU network and responsible for their operation.
- (7) The information technology administrator of the relevant TBU component part (hereinafter referred to as "administrator") is the employee authorized by the senior executive of the component part (Dean/Head/Director). The authorized employee is in charge of administration of computers in the relevant component part and of terminal systems in the departments of the component part.
- (8) The rules laid down in this Directive are binding on all users of the TBU network and apply to all computers and similar devices connected to the TBU network.

Article 2

Access rights to the TBU network and identification of users

- (1) All TBU employees and students shall have a user account established in order to access the TBU network. The account is established after the person (employee or student) has been included in the relevant registration (SAP, IS/STAG). In justified cases, the users may have several accounts in the TBU network. Each particular account involves certain access rights that specify the rights of users to access the TBU network sources.
- (2) A new user is assigned a user name and a password (login). The user is required to change his/her password.
- (3) The right to use the TBU network expires in case of termination of employment (employees) and termination of studies (students).
- (4) Students are allowed to use the TBU network only to a limited extent during the period of suspension of studies.

Article 3

General obligations of users

- (1) The users are allowed to use computers in the TBU network in accordance with their work and study-related duties, and that in particular for educational, scientific, research, development, innovation, artistic and other creative activities and tasks related to the operation and administration of TBU. They must, at the same time, strictly respect property rights over the data stored in electronic form.
- (2) It is not permitted to use the network for commercial purposes, for dissemination of commercial information, for political, religious and/or race campaigns, for promotion of drugs and to disseminate material which is contrary to the law.
- (3) When communicating with other networks, the users are required to observe the rules valid in these networks and the Access Policy (AP) for the CESNET Large Infrastructure, as amended (www.cesnet.cz).
- (4) All components of the TBU network are owned by TBU, or TBU has or exercises rights of use in relation to them. Theft and vandalism (damage) are unacceptable as regards the electronic form of data and information as well as the physical equipment itself.
- (5) The users are, in particular, required to:
 - a) Protect their user accounts with a non-trivial password, to keep this password confidential and not to disclose it to other users and/or to third parties.
 - b) Take care of the hardware which they use for connection to the TBU network, protect it against abuse and maintain the relevant software (particularly the operating system and protective programs) updated.
 - c) Take precautions to detect viruses or another harmful software and prevent their spread in the TBU network.
 - d) Inform the administrators of the TBU network about flaws detected in the security of the TBU network and about occurring hardware problems.
 - e) When using the services of computer networks, to avoid behaviour that might cause a nuisance to other network users.
- (6) The users are, in particular, not permitted to:
 - a) Connect any active elements (in particular routers, switches, access points, etc.) or servers

- to the TBU network without previously consulting the administrators of the TBU network and without their written consent.
- b) Connect such devices to the TBU network which do not meet the provisions of valid regulations and may endanger human health or life, damage the TBU network or another property and/or negatively influence the operation of the TBU network.
 - c) Interfere in any manner with the cables and interconnection elements in the TBU network, including their switching off without serious reasons.
 - d) Damage and/or to allow damage to or destruction of software and hardware equipment of the TBU network (computers, software as well as communication lines).
 - e) Without the TBU network administrators' consent, to install software programs which excessively increase the load on the TBU network and on the servers.
 - f) Without authorization, to use the TBU network to install, copy and/or publicly share the following items: Works, software, databases and other products of intellectual creativity which are protected by intellectual property right legislation (particularly by the copyright act, by act on personal data protection and by act on confidential information).
 - g) Make unauthorized copies even of parts of software and/or of data in relation to which TBU exercises property rights, or rights of use.
 - h) Make unauthorized modifications to programs, data and/or to technical equipment owned or used by TBU. Strictly forbidden are unauthorized modifications to the configuration of computers or of other devices which could influence the operation of the whole TBU network.
 - i) Knowingly use and spread files in any way infected and thus threaten the security of data in the TBU network.
 - j) Attempt to penetrate systems which the user is not authorized to use.
 - k) Provide access to the TBU network and to other services of the TBU network to other legal or physical entities.
 - l) Provide the assigned user name and the password to his/her account to another person. If a user provides the mentioned information to a person not entitled to access the network or to a person whose access has been locked for whatever reason, this is considered a gross violation of the rules.
 - m) Work in the network assuming false identity (including sending electronic mail under false identity) or take advantage of errors made by other users (e.g. failed logout, inappropriate protection of files) in order to access foreign data and/or information, and use such software that may result in the assumption of false identity.
 - n) Attempt to obtain access rights not assigned to them by the TBU network administrators (e.g. unauthorized access to any non-public information resources of TBU or of third parties). If a user finds a way to obtain access rights not assigned to him/her due to a software or hardware equipment error, he/she is required to inform the TBU network administrator about this fact without delay.
 - o) Secretly monitor the activities and to copy messages passing through the individual nodes of the network, unless this is done during the performance of such activity during specialized course units offered by a specialist department/studio; however, this activity must be carried out solely in laboratories of the same department, under conditions specified by the operator of the laboratory and with consent of the users concerned.
 - p) Use electronic means (particularly the electronic mail) to harass or intimidate other users.

This category also involves sending of chain letters, letters sent to addresses coincidentally selected in the TBU network, letters sent to addresses obtained from mailing lists compiled without consent of the addressees.

- q) Use the TBU computer devices to commit misdemeanours and criminal offences in contradiction to the valid laws.
- r) Use the TBU computer devices to do the activities mentioned in items above and directed against any other organization whose computer devices are available via the computer network.

Article 4

General rights and obligations of the ITC

- (1) The ITC is responsible for the operation of the TBU backbone network, for a functional connection of all TBU component parts, for the operation of central network services and servers. The ITC administers the address space and allocates addresses to the individual sub-networks.
- (2) The ITC gives methodological instructions about the rules for use of the TBU network to the administrators and cooperates with them during the provision of services of the TBU network according to the needs of the component parts, provided that requirements set out in this Directive have been fulfilled.
- (3) The ITC is entitled to keep records of TBU users. The ITC is in charge of the administration of their user accounts, e-mail addresses and of allocation of shared network disk space on central servers.
- (4) The ITC is entitled to monitor the operation of the TBU network. If there is a justified need to check as to whether the access to the resources of the TBU network is authorized, or in case of any other violation of this Directive, the authorized employee of the ITC may monitor the activity of a particular user following a decision taken by the Head of the ITC or by a superior authority.
- (5) The ITC is entitled to disconnect that part of the TBU network (sub-network) to which technical devices have been connected or where the configuration of the network software has been modified, both without consulting the ITC and the administrator respectively, and these devices or this modification have led to serious defects which may affect the operation or security of the TBU network.
- (6) The ITC is entitled to temporarily restrict access to services of the TBU network on reasonable suspicion of a violation of this Directive.
- (7) The ITC is entitled to immediately lock the relevant user account on reasonable suspicion of an abuse of the same user account. The ITC shall immediately inform the relevant superior of the respective component part or the Student Affairs Office and the Vice-Dean of the relevant faculty about the user account being locked.
- (8) The ITC is entitled to establish other binding rules regulating specific activities in the relevant sub-networks of the TBU network.

Article 5

Basic rights and obligations of administrators

- (1) The administrators are particularly entitled to:
 - Comprehensive services to be provided by the ITC and related to the operation of the TBU

network,

- Be informed by the ITC about the state of the tools used in the TBU network and about the development of the TBU network,
- Receive methodological assistance with problems related to the operation of the TBU network from the ITC administrators.

(2) The administrators are required to:

- Systematically collaborate with the ITC during the implementation of the provisions of this Directive.

Article 6

Sanctions to be imposed for non-observance of the rules for computer network use

- (1) The ITC administrator and the administrator are entitled to temporarily restrict, deny or refuse the access to the TBU network for users who provably violated the provisions of this Directive, and that within the limits of the rights and competences conferred.
- (2) An intentional infringement of the provisions of this Directive by students shall be considered as a disciplinary offence in compliance with § 64 of the Act No. 111/1998 Coll. on Higher Education Institutions and on Alterations and Amendments to Other Acts (Higher Education Act), as amended. In compliance with § 65 of the above-mentioned Act, a sanction may be imposed on a student for a disciplinary offence in compliance with the provisions of the Disciplinary Code which are relevant to students of Tomas Bata University in Zlín; in consequence of a particularly serious disciplinary offence which is committed intentionally or deliberately, the student may even be expelled from studies.
- (3) An infringement of provisions of this Directive by an employee shall be considered as a breach of basic professional duties (§ 301 Letter c) and d) of the Act No. 262/2006 Coll., as amended - Labour Code) and may result in relevant labour law consequences including termination of employment.
- (4) If a less serious breach of this Directive is detected, the TBU network administrator or a person authorized by him/her to act as his/her substitute is entitled to give the user a warning. In case of a gross violation of the rules, the TBU network administrator shall report the breach to the Head of the respective department in case of employees, or to the relevant Student Affairs Office and to the Vice-Dean of the relevant faculty in case of students.
- (5) This procedure neither restricts nor excludes any criminal responsibility.

Article 7

Final provisions

- (1) The ITC is authorized to monitor the observance of this Directive.
- (2) The rules for the TBU network use at a TBU component part may be amended by rules issued by the senior executive of the relevant component part. The rules for computer network use at a TBU component part must not contradict the provisions of this Directive.
- (3) This Rector's Directive replaces Rector's Directive No. 27/2011 issued on 19 October 2011 and its Annex No. 1 – Rector's Directive No. 16/2013 issued on 21 October 2013.