BRNO UNIVERSITY OF TECHNOLOGY

Date of issue:	1 May 2017
Effective date:	1 May 2017
Responsibility:	Computer and Information Services Centre
Binding for:	All components of BUT
Issued by:	Rector of BUT
Repeals:	Rector's Directive No 3/1999, Rector's Directive No 33/2004 and Bursar's Directive No 35/2001
Supplements:	-
Number of pages:	9
Number of annexes:	1

DIRECTIVE NO 22/2017

RULES OF OPERATION OF THE BUT COMPUTER NETWORK, BUT WI-FI NETWORK AND THE KOLEJNET NETWORK

PART ONE

BUT COMPUTER NETWORK

Article 1

Basic provisions

1. The BUT computer network is part of the Brno Academic Computer Network (BACN) built by higher education institutions and other organisations in Brno. It is directly connected to the national network for science and research and through it to the Internet.
2. The term computer network means all technical and software means that serve to connect computers and to use this connection. The mission of the computer network is to ensure the data connection of the BUT campuses and their connection to the BACN for the purposes of teaching, research and ensuring the operation of the university.
3. The rules set out in this Directive are binding on all users of the computer network and all computers and similar devices connected to the computer network. Where a section of the rules applies only to students, the term student is used. Where a section of the rules applies only to employees, the term employee is used. If the term user is used, the rule applies to employees and students.
4. The computer network administration is governed by the BUT Computer Network Administration Rules. These rules set out the rights and obligations of computer network administrators. The corresponding articles of these rules also apply to users who manage their own computing devices connected to the BUT computer network.
5. The rules of access to the BACN and other networks (TEN-ISS, Internet) are specified in the rules of operation of these networks.

Article 2

Access rights and identity

1. Only authorised users may use the BUT computer network. An authorised user (hereinafter the "user") is a user is demonstrably familiar with this Directive. The list of users is maintained by the relevant computer network administrator.
2. Employees and students of the BUT have the right to become users. Persons of other organisations may use the BUT computer network only on the basis of written permission issued by the Dean of the relevant faculty or the Rector or their authorised representatives.
3. Users are obliged to familiarise themselves with other up-to-date information and instructions available electronically (*http://www.vutbr.cz/rules*).
4. If the user's identity is required for access to the computer network, the user shall use the name assigned to him/her by the computer network administrator. The user is obliged to use a non-trivial password for identity verification and to keep this password secret to prevent its unauthorised use.
5. The user may not provide the assigned username and password to another person. It is considered a gross violation of the rules to provide these credentials to a person who is not entitled to access the network or whose access has been blocked.

6. The user may not take advantage of another user's negligence (e.g., failure to log out) to work under the identity of another.
7. User access rights are assigned by the computer network administrator. The user must not by any means attempt to obtain access rights that have not been granted to him/her. If the user obtains access rights that do not belong to him/her due to a system error, he/she is obliged to immediately report this fact to the administrator (at the level of the institute, campus, faculty or at cert@vutbr.cz) and must not exercise these rights.
8. The user may not abuse the BUT computer network to obtain unauthorised access rights to any information resources available through the BUT computer network.

Article 3

Use of the BUT computer network

1. The user may use the computer resources and computer network only for educational, scientific, research, development and artistic purposes or for tasks related to the operation and administration of the BUT. Violation of the rules is considered to be, in particular, use for commercial activities unrelated to the activities of the BUT, dissemination of commercial information, political, religious or racial agitation or propaganda, promotion of drugs and dissemination of materials that are contrary to the law.
2. The user has the right to use only legally acquired software. Copying of software is only permitted in compliance with applicable copyright laws. Shareware or freeware obtained through the BUT computer network may be used by the user only for the purposes specified in paragraph 1. Using the computer network to offer illegally obtained software or data is considered a gross violation of the rules.
3. The user may not interfere with software, data and technical equipment of the computer network without the consent of the administrator. Unauthorised changes to the configuration of computers or other resources that could affect the operation of the computer network are especially strictly prohibited. Students may not install software without the permission of the administrator.
4. The user has the right to use the allocated disk space, computing resources and computer network only with respect to the total load. The user must not knowingly interfere with the work of other users or the operation and performance of the network. The user must obey the instructions of the administrator to reduce the load generated by him/her without delay.
5. The size of transmitted e-mails and conferences may be limited. The specific limit is determined by technical possibilities and is set by the administrator. If the user's disk space limit is exceeded, the user may be automatically blocked from receiving further mail.
6. The BUT is not responsible for loss of user data in any way. The users are responsible for making backup copies of user data and software.

Article 4

Privacy protection and disclosure of information

1. The same rules apply to the use of electronic mail and conferences as to the use of normal mail; an email message shall have the nature of an open letter.

2. The user is obliged to ensure that his/her messages are accurately addressed and that there is no unwanted harassment of other users caused by chain messages or messages addressed to mailing lists collected without the consent of the addressee.
3. The user is obliged to use the assigned username (mailbox name) when sending electronic mail. It is considered a gross violation of the rules to send messages under false identities for the purpose of fraud, intimidation and obtaining unauthorised information.
4. The receipt of electronic mail from addresses that violate the provisions of Article 4(2) and (3) may be blocked.
5. The user bears full legal responsibility for the content of his/her own publicly available WWW pages and other information resources, especially for violation of copyright law when copying other people's materials.
6. Files in user directories and system mailboxes are the private data of their owners. Users are entitled to privacy protection, even if they do not protect their directories. Copying data of another and intercepting traffic on a computer network to obtain the content of messages or data is considered a gross violation of the rules.
7. The administrator has the right to render inaccessible files that are in violation of Article 3 or jeopardise the security of the system and computer network (infected software, tools for eavesdropping, obtaining rights of another, etc.), and the user is obliged to remove them immediately at the administrator's request.
8. The BUT is not responsible for possible misuse of data during transmission and storage of information on the computer network.
9. The administrator shall have the right to perform all acts necessary for the performance of his/her function, including, where applicable, the control of data and the monitoring of user activity. If the user uses encryption to keep information confidential, he/she shall, in case of doubt as to its use within the meaning of Article 3, make the contents of the data available to the administrator.

Article 5

Rules for connection to the computer network

1. The user is obliged to request the consent of the network administrator as follows:
   a) before connecting a device to the computer network;
   b) before changing the configuration of a device that could affect the network' operation;
   c) before permanently disconnecting a device from the computer network.

   The administrator registers connected devices in accordance with the internal ordinance governing the administration of the BUT computer network.
2. The proper installation of the operating system and network software on a computer connected to the computer network is the responsibility of either an authorised employee designated by the network administrator or the user, if the user is allowed to install the operating system independently (i.e. if permitted by the Computer Network Operating Rules at the level of the relevant faculty or institute).
3. When independently administer the operating system and network software of a computer connected to the computer network, the user must comply with the relevant provisions of the BUT Computer Network Administration Rules.
4. The user must not use a network address other than the one assigned to him/her (either automatically or statically) to connect to the computer network.

5. Modems and other means for external access to the BUT computer network may be operated by the user only with the consent of the administrator.
6. The use of the BUT computer network within the framework of scientific and pedagogical cooperation with other organisations is possible only on the basis of a written permission issued by the Rector or the Dean of the relevant faculty.

Article 6

Penalties for students for non-compliance with the computer network operation rules

1. Violation of the rules of operation of the computer network is considered a violation of the rules within the meaning of Section 62(1)(g) of Act No 111/1998, on higher education institutions and amending and supplementing other acts (Higher Education Institutions Act).
2. In accordance with Sections 64 to 67 of the above Act, a student may be sanctioned in accordance with the Disciplinary Rules, and for a particularly serious violation, the student may be expelled from the Studio.
3. A detected minor violation of the computer network operation rules gives the network administrator or his/her designee the right to reprimand the student.
4. In the case of more serious violations or repeated minor violations of the rules, the administrator or a person authorised by him/her may withdraw the student's right to freely use the services of the computer network outside of organised study classes for a predetermined period of time (maximum two calendar months). In this case, the student has the right to appeal to the Dean (in the case of a faculty) or the head (director) of the relevant component of the BUT (e.g. dormitories and canteen). This appeal shall not have suspensive effect.
5. In the event of a repeated or particularly serious breach of the rules, the case will be dealt with as follows:
   a) on the day the violation of the network rules is discovered, the student loses the right to use the computer network services;
   b) the case is referred to the Disciplinary Committee of the relevant faculty of the BUT;
   c) based on the Disciplinary Committee's deliberations, the Dean of the relevant faculty decides on the imposition of a sanction – this may also be the denial of BUT computer network services for a predetermined period of time.

   Possible criminal liability is neither limited nor excluded by this procedure.

Article 7

Penalties for employees for non-compliance with the computer network operation rules

1. Violation of the provisions of this Directive by employees shall be considered a violation of the employee's basic duties [Section 73(1)(c) and (d) of the Labour Code] and may result in appropriate labour-law consequences, including termination of employment.
2. When a violation of the rules of operation of the computer network is detected, the network administrator or a person authorised by him/her shall notify the employee who has violated the rules, or in the case of a gross violation of the rules, the relevant head of the department of this fact.
3. In the event of a repeat violation, the case will be dealt with as follows:

a) on the day the violation of the network rules is discovered, the employee loses the right to use the BUT computer network services;
b) the case is forwarded to the Dean of the relevant BUT faculty or to the Rector in the case of other BUT components, who then decides on a labour-law action.

Possible criminal liability is neither limited nor excluded by this procedure.

Article 8

Other provisions

1. The users undertake to comply with the principles set out in this internal ordinance by signing the User Account Assignment Report, thereby acknowledging the penalties that result from non-compliance with the rules.
2. The rules of computer network operation at the level of the faculty or other BUT components may be supplemented by rules issued by the Dean of the respective faculty or the head of the respective BUT component (e.g. dormitories and canteens). The rules of operation at the level of the faculty and other BUT components must not conflict with the BUT Computer Network Operation Rules.

PART TWO

BUT WI-FI NETWORK

Article 9

Definitions

1. The BUT Wi-Fi network is a set of technical means and equipment enabling access to the BUT computer network via wireless network connection devices or by other technical means defined in this Directive.
2. A user of the BUT Wi-Fi network (hereinafter the “user”) is any person who meets the conditions laid down in Article 2 of this Directive.
3. The Wi-Fi access gateway of the BUT network is a technical device enabling access of authorised users from the BUT Wi-Fi network to other parts of the BUT computer network and to networks connected to it.
4. Local Wi-Fi network is the part of the BUT Wi-Fi network that includes access points for connecting end devices and devices connected to this network within one faculty, BUT component or site.

Article 10

Users

1. The user connecting the end device to the BUT Wi-Fi network is obliged to follow the administration rules of this Device defined by the internal ordinance governing the administration of the BUT computer network.

2. The user is required to use DHCP to be assigned an IP address. Setting a static IP address is considered a gross violation of the BUT Wi-Fi network rules.

3. The authorisation and identity of the user for access to other parts of the BUT computer network is verified on the basis of the name and password assigned for access to the BUT central information system (BUTLogin and BUTPassword).

4. When using the BUT Wi-Fi network, users shall also obey Part One of this Directive and the operating rules of the relevant facility or part thereof. In case of violation of these rules, the administrator of the local Wi-Fi network may temporarily withdraw the access right to the BUT W-Fi network. The user shall request the appropriate local Wi-Fi network administrator or the local Wi-Fi network administrator of his/her faculty to restore access. Any other penalties arising from other regulations shall not be limited or excluded by this.

5. End devices connected to the BUT Wi-Fi network must be adequately secured by appropriate system configuration, the application of security patches, etc. In the case of an insufficiently secured or infected end device, the local Wi-Fi network administrator may temporarily revoke the access right to the BUT Wi-Fi network.

7. It is forbidden to run any server applications on the BUT Wi-Fi network. The operation of these applications is limited at the Wi-Fi access gateway. The BUT Wi-Fi network itself is not secured against eavesdropping. For secure access from the Wi-Fi network, it is recommended to use encrypted channels (e.g. via SSL, SSH or VPN server). Under no circumstances is it advisable to transmit sensitive information in open form.

Article 11

Administration of the BUT Wi-Fi network

1. Data transport between the access points and the access gateway is ensured by the BUT computer network. The correct configuration of the individual parts of the BUT computer network is always the responsibility of the administrator of the relevant part of the network.

2. The administrator of the local Wi-Fi network is methodologically subordinate to the administrator of the faculty network.

3. The administrator of the local Wi-Fi network is a member of the Council of Network Administrators.

4. In the event that a local Wi-Fi network administrator is not appointed, his/her duties are transferred to the faculty network administrator.

5. The Wi-Fi access gateway is administered by the CVIS.

Article 12

Rights and obligations of Wi-Fi network administrators

1. Local Wi-Fi network administrator:

   a) Collaborates with faculty, campus and local network administrators in the deployment of the Wi-Fi network;
   b) installs, configures and manages Wi-Fi access points;
   c) maintains a list of access points and their configuration parameters;
   d) informs the users about access points and Wi-Fi network parameters;

e) provides technical support to users of the Wi-Fi network related to the operation of the Wi-Fi Network.

2. The administrator of the Wi-Fi network access gateway (in the event that such is not designated, these responsibilities are transferred to the administrator of the BUT backbone network):

a) ensures the operation of the Wi-Fi network access gateway;
b) ensured automatic address allocation operation via DHCP for local Wi-Fi networks;
c) ensures the operation of the VPN concentrator for the needs of the BUT Wi-Fi network;
d) defines the Wi-Fi network security policy in cooperation with the Council of Network Administrators;
e) allocates address space to local Wi-Fi networks in cooperation with the administrator of the backbone network;
f) cooperates with the backbone network administrator to connect local Wi-Fi networks at the backbone level;
g) cooperates with the administrator of the central authentication service of the BUT (CAS BUT).

Article 13

Wi-Fi network access points

1. Access point administration addresses are allocated from the private address space or from the address space allocated to the faculty.
2. The technical parameters for the operation of access points shall be set by the Council of Network Administrators.
3. Access points must be installed so that they cover only the internal part of the BUT buildings.
4. Alternatively, an Ethernet connection can be used to connect to the BUT Wi-Fi network. In this case, the conditions of operation specified in this Directive shall also apply to the connection.
5. This Directive does not apply to the operation of access points that are not integrated into the BUT Wi-Fi network. These access points can be operated with different technical parameters and are considered an ordinary part of the BUT computer network, which is governed by an internal ordinance regulating the administration of the computer network.
6. It is advisable to mark the places covered by the Wi-Fi signal of the BUT Wi-Fi network with the BUT Wi-Fi network logo (see Annex – BUT Wi-Fi network logo), contact information for the administrator of the relevant part of the Wi-Fi network and basic technical information necessary for connection.

PART THREE

KOLEJNET NETWORK

Article 14

Basic provisions

1. Kolejnet is a computer network built on the BUT campuses for the needs of students. It consists of connections in computer rooms (Kolejní2 and Purkyňova 93) and connections in students' rooms.

Through the Brno Academic Computer Network (BACN), it is connected to the national network for science, research and education (CESNET 2) and through it to the Internet.

2. A user is any person who meets the conditions laid down in Article 2 of this Directive and accesses the resources of the BUT computer network.
3. A user who has concluded a connection contract with KaMB (dormitories and canteens of BUT) becomes a user of the connection.
4. Device registration means the process whereby the user of the connection enters information about the device(s) to be connected.

Article 15

Kolejnet users

1. Each user shall be demonstrably familiar with this Directive.

Article 16

Connection users

1. Based on the contract, the user is entitled to use a single connection and IP address, which is assigned automatically via DHCP or by the network administrator.
2. Immediately after a new device is first connected to the network, you must register it via a web browser. The registration results in a notification that the device is connected to the network, which includes the network address assigned to the user and other necessary information. The registration does not affect the duration of the connection contract. A maximum of 3 devices sharing a single network address can be registered per contract. Devices cannot be connected to the network at the same time.
3. Only the data outlet designated by the registration may be used to access the network. The connection to this data outlet cannot be changed without the administrator's knowledge.
4. It is forbidden to connect any device to the network without prior approval of the administrator or registration, except for the first registration of an unregistered device (computer). This rule also applies to devices that are not directly connected to the BUT computer network, but may nevertheless use the BUT computer network resources.
5. When administering the equipment connected to the network, the user of the connection is obliged to comply with the internal ordinance governing the administration of the BUT computer network. The rules may be supplemented or clarified by regulations and recommendations of the network administrator, which are applicable to the Kolejnet network and are available in electronic form at: (http://www.kn.vutbr.cz/rules/).
6. The user of the connection is obliged to prevent anyone who is not familiar with this Directive from using the resources of the BUT computer network.
7. The user of the connection is responsible for misuse of the equipment connected to the network.

Article 17

Other provisions

1.ZThe connection may be used by the user of the connection only on the basis of a contract for connection to the computer network concluded prior to the use.

PART FOUR

FINAL PROVISIONS

Article 18

Final provisions

1. This internal ordinance shall take effect on the date specified in its heading.
2. Updates to Annexes of this internal ordinance will be made after the approval of the submitted change by the issuer of the ordinance. The updated Annex will be published by posting on a specific effective date.

Prof. RNDr. Ing. Petr Štěpánek, CSc.

Rector