Code:	SR/13/2025	
Ref. No.:	UTB/25/018649	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Communication Network Security Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	7 April 2025	Version: 01
Effective from:	1 May 2025	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services, Data Protection Officer	
Pages:	7	
Appendices:	0	
Distribution list:	Tomas Bata University in Zlín	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) The Communication Network Security Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* defines the methods of protecting the communication and data network (hereinafter referred to as the "TBU network") in accordance with the Act No. 181/2014 Coll., on Cyber Security, and on Amendments to Related Acts, as amended (hereinafter referred to as the "Cyber Security Act") and Decree No. 82/2018 Coll. on Security Measures, Cyber Security Incidents, Reactive Measures, Requirements on Documents Submitted in the Area of Cyber Security and Data Destruction (hereinafter referred to as the "Decree on Cyber Security") at Tomas Bata University in Zlín (hereinafter referred to as "TBU").

(2) The purpose of this policy is to determine how to protect the TBU network to ensure proper and secure operation.

(3) The individual terms used in this Directive are defined particularly by the Cyber Security Act and the Decree on Cyber Security. The individual terms are listed in the document entitled '*Glossary of Cyber Security Terms',* which is available on the TBU website in the *Cyber Security* section.

Article 2
TBU network

(1) TBU operates and manages a non-public network for the transmission of digital data to provide its own electronic services and to provide access to internal and external digitized resources.

(2) The term "TBU network" refers to all technical and program tools serving for connection of devices 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.

(3) The TBU network is connected to the Internet via the national e-infrastructure for science and research operated by CESNET z. s. p. o., of which TBU is a member.

(4) The term "users of TBU network" (hereinafter referred to as "users") refers to:

a) TBU students (hereinafter referred to as "students") and employees with a concluded employment contract or agreement on work performed outside regular employment (hereinafter referred to as "TBU employees"), who have established a user account for access to the TBU network and directly use the aforementioned TBU networks or devices connected to them,
b) Emeritus Professors, scholarship holders, guests and other users who use the TBU network on the basis of relevant roaming or other agreements,
c) employees of major suppliers and third parties under contractual arrangements for the provision of services or products, as appropriate.

(5) The term "user account" (hereinafter referred to as "account") refers to the authorization to use a particular device or the TBU network; each user has a unique user identification. Usually, it is a user name and a password.

Article 3
Access rights to the TBU network and identification of users

(1) Each user referred to in Article 2, Paragraph 4 Clause a) shall have an account for access to the TBU network. The account shall be created on the basis of the user's entry in the relevant register (SAP, IS/STAG). In justified cases, users may have more than one account in the TBU network.

(2) The new user is automatically assigned a username and password (login). Each user is obliged to change this assigned access password.

(3) The user's right to use the TBU network shall cease upon termination of employment, contract/agreement, termination or suspension of studies.

Article 4
Definition of rights and responsibilities of TBU network users

(1) The users are allowed to use the TBU network in accordance with their work and study 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) Employees of major suppliers and third parties may use the TBU network solely for the performance of their obligations under contracts for the provision of services or products.

(3) It is forbidden to use the TBU network for commercial purposes, for the dissemination of commercial information, for political, religious and/or race agitation, for the promotion of drugs and for the dissemination of material which is contrary to the law.

(4) When communicating with other networks, the users are required to observe the rules valid in these networks and the *CESNET Access Policy*, as amended (www.cesnet.cz).

(5) 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.

(6) The users of the TBU network are, in particular, required to:

a) Protect their user account with a password in accordance with the *Safe User Policy*.
b) Protect the technical means they use to connect to the TBU network from misuse and keep the software used on them (especially the operating system and protection programs) up to date.
c) Act in such a manner as not to cause the introduction of malicious software into the TBU network and its spread.
d) Inform the TBU network administrator of any detected shortcomings in the security of the TBU network and of any hardware defects.
e) Avoid generating excessive data flows that cause a load on the TBU network.

(7) Users of the TBU network are forbidden, in particular, to:

a) Connect any active elements (in particular routers, switches, access points, etc.) or servers to the TBU network without previously consulting the administrator of the TBU network and without his/her 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.
e) Without the TBU network administrator’s 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, computer programs, 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 the Act on the Protection of Classified Information and Security Eligibility 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 software, 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 or security of the whole TBU network.

i) Knowingly use and spread infected files in any way 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 unauthorized physical or legal 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 TBU 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. 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 his/her direct superior about this fact without delay.
o) Eavesdrop on traffic and make copies of messages passing through individual network devices, unless such activity is carried out in the context of the teaching of specialised course units by a specialist department/studio, which must be carried out exclusively on the premises of that department/studio designated for that purpose and under conditions to be determined by the individual teacher or the guarantors of the course units taught.
p) Use the resources of the TBU network for the activities listed in a) to o) against any other organization whose communication resources are accessible via the TBU network.
q) Use the TBU network in violation of applicable laws and to commit misdemeanours and crimes.

Article 5
Definition of rights and responsibilities for the secure operation of the TBU network

(1) According to the *Organizational Regulations of the TBU Rectorate*, as amended, the Information Technology Centre (hereinafter referred to as the "ITC") is responsible for the administration of the TBU network.

(2) The administrator of the TBU network (hereinafter referred to as the "network administrator") is the person or persons in charge of the administration of the TBU network resources and their operation.

(3) The ITC is responsible for the operation of the TBU backbone network, for a functional connection of all TBU constituent parts, for the operation of central network services and servers. The ITC administers the address space and allocates addresses to the individual sub-networks.

(4) The ITC gives methodical instructions about the rules for use of the TBU network to the IT administrators and cooperates with them during the provision of services of the TBU network according to the needs of the constituent parts.

(5) The ITC keeps 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.

(6) The ICT is entitled to:

a) Disconnect a part of the TBU network (subnetwork) to which unapproved technical resources have been connected or on which an unapproved change in the configuration of network software has been made, and these resources or this change have caused serious malfunctions that threaten the operation or security of the TBU network.
b) Temporarily restrict access to TBU network services if there is a reasonable suspicion of a breach of this Directive.
c) Block the user account immediately if there is reasonable suspicion of misuse of the user account. The ITC shall immediately forward the information on the blocking of the user account to the direct superior or the Student Affairs Office of the Faculty concerned and the relevant Vice-Dean, and in the case of users referred to in Article 2, Paragraph 4, Letters b), c), to the Head of the constituent part concerned.
d) Establish other binding rules governing specific activities in individual subnetworks of the TBU network.

Article 6
Rules and procedures for ensuring the security of the TBU network

(1) Each part of the TBU network shall be documented at the physical and logical layers to ensure its security and resilience to potential cyber-attacks.

(2) The management of the TBU network and network elements shall be separated from the management of workstations and servers.

(3) The TBU network shall be segmented and logically separated to ensure security and resilience to potential cyber-attacks.

Article 7
Network access control rules and procedures

(1) Access control policies shall be applied to all segments of the Local Area Network (LAN) under the administration of TBU.

(2) Identity management and authentication tools shall be used for user and administrator access to the TBU network, and technical resource access to the TBU network shall be managed using technical resource access management tools.

(3) Access shall be controlled on the basis of groups and roles.

Article 8
Rules and procedures for network monitoring and evaluation of operational records

(1) The ITC shall monitor the operation of the TBU network and, in justified cases, may also monitor the activity of a specific user.

(2) Event logs shall be kept for the period required by specific legislation (Decree on Cyber Security), but at least for 12 months.

(3) Event logs shall be secured against unauthorized access and unauthorized modification.

(4) All elements of the TBU network shall be connected to a designated source of accurate time and shall be synchronised at least once a day.

(5) Evaluation of the operational records shall be the full responsibility of the ITC.

Article 9
Rules and procedures for protecting remote access to the TBU network

(1) Remote user access to the TBU network shall be enabled through a communication channel protected by cryptographic means.

(2) Access from external networks shall only be possible through demilitarised zones (DMZ) designed to ensure that an external attack does not compromise the security of the internal network.

(3) The remote connection of suppliers is only possible on the basis of contractual relationships, which include a mutually accepted security policy for such connections.

(4) Secure remote access to internal networks shall be documented and governed by the following rules:

a) Users shall only use the Virtual Private Network (hereinafter referred to as "VPN") operated by TBU for remote access.
b) The same rules set out in the cybersecurity policy shall apply to the use of remote access as apply to on-site work.
c) The connection established within the remote access is encrypted and is preceded by user authentication.
d) Accesses shall be uniquely recorded together with the user's identification.
e) Users shall not share their remote access rights.

(5) Users of remote access resources shall promptly perform all recommended updates and modifications to remote access resources to minimize the risk of misuse for unauthorized access.

Article 10
Sanctions to be imposed for non-compliance with TBU network rules

(1) The TBU network administrator and the IT administrator are entitled to temporarily restrict, deny or cancel 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) If a minor violation of this Directive is discovered, it shall entitle the network administrator or the person authorized by him/her to notify the user of the violation.

(3) 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.

(4) An infringement of the 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.

(5) Any criminal liability shall not be restricted or excluded by this procedure.

Article 11
Final provisions

(1) This Directive shall abrogate and replace the Rector's Directive No. 1/2016 and the Rector's Directive No. 2/2016.

Document version			
Date	Version	Changed	Description of change
7 April 2025	01	CS Manager	Creation of document

This English version of the internal regulation is not legally binding; it is for informational purposes only and does not have to correspond to the Czech version of the document.