Code:	SR/5/2025	
Ref. No.:	UTB/25/006076	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Safe User Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	13 February 2025	Version: 01
Effective from:	1 March 2025	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services, Data Protection Officer	
Pages:	4	
Appendices:	0	
Distribution list:	TBU employees	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) The Safe User Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* establishes rules for user behaviour to ensure information security and reduce the risk of a cyber security incident and cyber security breach 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 define the principles of secure user behaviour, to set out the obligations of users and to define the rules for the secure operation of important information systems (hereinafter referred to as "IIS"). The term "users" refers to students, employees with a concluded employment contract or agreement (hereinafter referred to as "TBU employees"), Emeritus Professors and scholarship holders under concluded cooperation agreements and, where applicable, employees of major suppliers and third parties under a concluded contractual relationship for the supply of services or products.

(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
Rules for the safe handling of IIS assets

(1) The rules for the treatment of IIS assets shall be determined by their classification and shall be documented for each asset in accordance with the asset classification set out in *Annex 1* to the Rector's Directive on *Asset Management Policy*, as amended.

(2) Users are obliged to store, save and archive the information, data and processes specified in Paragraph 1 in such a way as to ensure that they are adequately protected against unauthorised access and to prevent their misuse.

(3) Each user is obliged to:

a) lock his/her open access/active login endpoint device (to IIS assets) whenever he/she leaves the workplace,
b) terminate active access (logout) to all IIS assets at the end of his/her work shift.

(4) Each user shall have access only to those assets of the IIS that he/she needs to perform his/her activities.

(5) Any exceptions to the rules shall be made on the basis of a reasoned and approved request. The request shall be approved by the applicant's immediate superior and the Head of the relevant component part and forwarded to the Cyber Security Manager (hereinafter referred to as the "CS Manager"), who shall approve or deny the request. If the CS Manager approves the request, it shall be forwarded to the Director of the TBU Information Technology Centre (hereinafter referred to as "ITC") for technical implementation.

Article 3
Secure password use

(1) For the purposes of this policy, the term "password" refers to a combination of characters and/or numbers, including a PIN.

(2) Users must store and use passwords in such a way that they are not disclosed to others.

(3) Passwords used for access to TBU information systems must not be used by the user for services, applications and systems used for private purposes.

(4) Users shall be informed of the current parameters of the individual strong password creation rules during registration or when changing their password.

(5) Password creation rules shall specify at least the following parameters:

a) minimum password length,
b) the use of a combination of lower case, upper case, numerals and special characters,
c) the possibility to change the password on request,
d) mandatory password change after a certain period of time,
e) prohibition of creating a password from a fact that can be easily guessed or obtained from personal information, e.g. first name, last name, date of birth, birth number, etc., not susceptible to dictionary attack (i.e. passwords not made up of words from a dictionary), not matching the login name,
f) inability to reuse the same password when changing it.

(6) Rules for password creation and use may be enforced directly by the system.

Article 4
Safe use of e-mail and internet access

(1) The following rules apply to electronic mail:

a) Information contained in electronically transmitted messages must be protected in accordance with the *Asset Classification at TBU.*
b) Users shall only use electronic mail for study and/or work purposes.
c) Cryptographic means are required to protect information with a high level of confidentiality.

(2) When using electronic mail, it is prohibited to:

a) use TBU electronic mail for private purposes,
b) TBU employees are prohibited from using public e-mail services (e.g. Gmail, Seznam, etc.) for work purposes,
c) send unprotected personal or sensitive data via plain e-mail, including unencrypted attachments containing personal or sensitive data,
d) open attachments and web links in emails from unknown or untrusted sources; in the event of a suspicious email, the user is obliged to report this to the helpdesk at abuse@utb.cz,
e) set rules for automatic forwarding of e-mail outside TBU.

(3) Prior to the termination of the employment relationship or agreement, the TBU employee is obliged to ensure that his/her personal e-mail box (user@utb.cz) is set for automatic reply with the contact details of the employee's immediate superior and to delete the entire contents of the e-mail box no later than the date of the termination of the employment relationship or agreement. The day after the termination of the employment or agreement, the mailbox will be automatically blocked and deleted after 60 calendar days.

(4) Where a terminated or contracted employee has had access to a general email account generated by TBU, the immediate chief executive is responsible for ensuring that it is set up correctly, including changing access details.

(5) In connection with Internet access, the following activities are prohibited:

a) use Internet services for purposes other than study and work,
b) store IIS assets on unapproved public storage facilities in accordance with the Rector's Directive on the *Protection and Processing of Personal Data*, as amended,
c) download executable files and files containing macros from untrusted and unverified sources.

Article 5
Secure remote access

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

a) users must use only the Virtual Private Network (hereinafter referred to as "VPN") operated by TBU for remote access to IIS assets,
b) the use of IIS assets via remote access shall be subject to the same rules as those applicable to work in the workplace, as set out in the cybersecurity policies,
c) the connection established during remote access shall be encrypted and subject to user authentication,
d) accesses shall be uniquely recorded together with the user identification,
e) users shall not share their remote access rights.

(2) Users of devices enabling remote access shall promptly perform all recommended updates and modifications to devices enabling remote access to minimize the risk of misuse due to unauthorized access to IIS assets.

Article 6
Staying safe on social media

(1) Users whose job description does not include the use and management of official TBU social media accounts are not authorized to access social media.

(2) Users whose work involves the use and management of official TBU social media accounts shall observe the rules of safe social networking; in particular they shall:

a) protect login data, keep passwords sufficiently complex, confidential and change them regularly,
b) use social networks only for official TBU purposes and share only information that is consistent with the official communication policy, privacy policy and interests of TBU,
c) use a virtually separate environment or user profile.

Article 7
Security in relation to mobile devices

(1) Security in relation to mobile devices is governed by the Rector's Directive – *Policy for Safe Use of Mobile* Devices, as amended.

Document version			
Date	Version	Changed	Description of change
13 February 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 original document.