Code:	SR/4/2025	
Ref. No.:	UTB/25/006075	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Secure Information Transfer and Exchange 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:	5	
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 Secure Information Transfer and Exchange Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* lays down rules and procedures for the protection of information transmitted, the means of protecting the electronic exchange of information and the rules for the use of cryptographic protection 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) This policy shall apply to all users and information assets, and the term "users" refers to students, employees with a concluded employment contract or agreement on work performed outside regular employment (hereinafter referred to as "TBU employees"), Emeritus Professors and scholarship holders under concluded cooperation agreements.

(3) Where appropriate, this policy shall also apply to employees of major suppliers and third parties under a concluded contractual relationship for the supply of services or products.

(4) 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 and procedures for the protection of transmitted information

(1) Procedures and measures shall be established to protect the transmission of information through all types of communication devices based on the Asset Classification specified in *Annex 1a* and the Asset Handling in *Annex 1b* to the Asset Management Policy, as amended.

(2) The transfer of information with external entities (e.g. contracting parties) must be in accordance with the *Supplier Management Policy*, as amended.

(3) The guarantor of the relevant asset, whose asset is shared with the contracting party, shall be responsible for the factual accuracy of the content of the contract concluded with the supplier, in accordance with the Bursar's Decree – *Preliminary Management Control before the Conclusion of a Contract*, as amended.

Article 3
Methods for the protection of electronic information exchange

(1) In order to protect electronically transmitted information measures shall be applied in accordance with the *Asset Management Policy*, as amended; and the following measures are applied at TBU:

a) the internal technical means of the relevant information system (IS/STAG – Information System for Studies Administration, e-Spis – Electronic Records Management System, SAP - Information System for Financial Management and other systems);
b) shared file system repositories with controlled access by authorised staff;
c) password-protected email attachments if they contain personal data, special categories of personal data or confidential data;
d) the Cesnet Filesender service provided by CESNET z. s. p. o. for the transfer of large data files (https://filesender.cesnet.cz/).

(2) Measures are applied to protect the media of electronically transmitted information in accordance with the *Asset Management Policy* and the *Policy for Safe Use of Mobile Devices*, as amended.

(3) Only information permitted by the Asset Handling in *Annex 1b* to the *Asset Management Policy*, as amended, may be made publicly available.

(4) The publication of information on the (electronic) official board of TBU is governed by the relevant legal provisions and is the responsibility of the authorised employee of the component part.

(5) The use of public Internet storage platforms (e.g. Google Drive, Microsoft OneDrive, Dropbox, etc.) for the transmission of information is prohibited.

Article 4
Rules for the use of cryptographic protection

(1) Cryptographic measures shall be used where necessary to ensure the confidentiality, integrity and availability of information transmitted in accordance with the Asset Classification set out in *Annex 1a* and the Asset Handling set out in *Annex 1b* to the *Asset Management Policy*, as amended.

Article 5
Rules for the use of electronic mail at TBU

(1) Electronic mail is used to communicate and exchange files via email messages.

(2) Each user referred to in Article 1, Paragraph 2, has a personal email address generated by the University (hereinafter referred to as "personal email address"), which is considered to be one of the official contacts of the user.

(3) The use of electronic mail and electronic conferences shall be subject to the same rules as the use of ordinary paper mail on the basis of Article 13 of the *Charter of Fundamental Rights and Freedoms* and Act No. 127/2005 Coll. on Electronic Communications, as amended. Email, if not encrypted, is to be understood as open letter mail.

I Creation and validity of personal email addresses

(4) A personal email address shall be set up automatically:

a) to TBU employees registered in the SAP information system,
b) to students who have at least one "active student status" in the IS/STAG information system.

(5) In addition, personal email addresses may be set up for Emeritus Professors and scholarship holders on the basis of cooperation agreements and shall be valid for the duration of the agreements.

(6) Users' personal email addresses shall remain functional for the duration of the employment or agreement or study.

II Email address format

(7) TBU uses the second-level domain "utb.cz" for electronic mail. Individual component parts of TBU, student organisations, on the basis of a contractual relationship or some other constituent parts have been allocated third-level domains in the form of "xxx.utb.cz". A list of these domains is available on the website of the Information Technology Centre (hereinafter referred to as "ITC") at cvt.utb.cz (hereinafter referred to as "ITC website"). New second-level and third-level domains may be created only for objective reasons and shall be created by the ITC.

(8) The user's personal email address is in the format user@utb.cz, where *user* is the assigned username to the TBU communication and data network.

(9) For specific communication and service management purposes, a different email address format may be used within second-level and third-level domains. A specific address format

will be determined by the ITC on the basis of a reasonable request from a user, approved by the immediate superior in accordance with the *Safe User Policy*.

(10) Email addresses may also be set up under other second-level domains owned by TBU. These addresses are set up by the ITC upon request and are subject to the same rules as addresses under the utb.cz domain.

III Use of electronic mail

(11) Users are entitled to use only the assigned email addresses and email inboxes (personal and specific) and shall be fully responsible for them. Users are obliged to keep secret their access data (especially password) used to access the email address.

(12) The email address is intended for communication on work and study matters.

(13) Users shall ensure that their messages contain a subject line, are correctly addressed and do not unreasonably harass other users by sending unnecessary bulk messages or messages sent to mailing lists that have been collected without the consent of the addressee.

(14) When communicating via electronic mail, the following activities are prohibited:

a) Sending electronic messages with false or fraudulent identities (phishing) and anonymous messages;
b) sending unsolicited advertising messages (spam) in accordance with Act No. 480/2004 Coll. on Certain Information Society Services and on Amendments to Certain Acts. Such messages may be sent only to persons who expressly request them;
c) sending messages containing files with malware and other dangerous programmes;
d) harassment of any kind (language style, frequency, size of messages, sending chain messages, etc.);
e) the use of vulgarisms or other inappropriate phrases that may damage the reputation of TBU;
f) attempting to hack into the user and email accounts of other users and violating in any way the applicable laws of the Czech Republic, internal rules and regulations of TBU and good manners.

(15) Failure to comply with the prohibition may be considered a disciplinary offence in accordance with the TBU Disciplinary Code in the case of students, a breach of employment obligations in the case of employees with all the consequences under labour law, and a breach of contractual arrangements in the case of third (contractual) parties, which may be sanctioned in the manner specified in the relevant contract.

(16) Users are obliged to be cautious when opening messages and their attachments, especially those from unknown senders. If users are unsure, they should contact the IT Administrator at their component part or the ITC. It is the responsibility of direct superiors to educate users about the threats associated with the use of email.

(17) Users are required to regularly read/check their inbox from their assigned email address.

(18) The size of transmitted email messages may be limited.

(19) Detailed information on TBU's electronic mail can be found on the ITC website.

IV Bulk email addresses

(20) Bulk email addresses can be set up for sending messages to groups of users within the TBU communication and data network. More details can be found at https://www.utb.cz/cvt/email-lists/.

(21) Bulk email addresses are intended for internal use only; the messages sent must be directly related to the mission or activities of TBU.

Article 6
Final provisions

(1) The provisions of Article 2 of this Directive shall also apply to the transmission and exchange of information in paper form.

(2) This Directive shall abrogate and replace the Rector's Directive No. 7/2017.

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.