Code:	SR/13/2024	
Ref. No.:	UTB/24/007646	
Category:	INTERNAL	
Type of document:	RECTOR'S DIRECTIVE	
Title:	Operation and Communication Management Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	2 May 2024	Version: 01
Effective from:	3 May 2024	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Legal Services, Information Technology Centre	
Pages:	3	
Appendices:	1	
Distribution list:	TBU employees	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) The Operation and Communication Management Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* establishes procedures and protocols to support effective asset management 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 ensure reliable, stable and secure operation of important information systems (hereinafter referred to as "IIS") and supporting assets in such a manner as to guarantee the security of primary assets.

(3) This policy shall apply to information assets created or used within the IIS, and to users of such assets.

(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
Powers and responsibilities associated with safe operation

(1) In accordance with Article 1, Paragraph 2 of this Policy, the Director of the Information Technology Centre is responsible for the management of the IIS operation. This responsibility can be delegated to appointed guarantors of primary and supporting assets.

(2) The Manager for Cyber Security (hereinafter referred to as the "CS Manager") is responsible for operational security and, in particular, cyber security management.

Article 3
Safe operating procedures

(1) Working methods are created for the management, administration and monitoring of the IIS assets, which are included in the operational documentation. The working methods are available to all employees concerned. The relevant Primary Asset Guarantor is responsible for keeping operational documentation, which is a confidential document.

(2) Safe operating procedures include, in particular:

a) Rights and obligations of employees who are users of the IIS in specifically defined roles as specified in *Appendix 1*, including administrators;
b) procedures for opening and closing of the IIS, for restarting or reloading of the IIS after failure and for dealing with error conditions or unusual incidents;
c) procedures for monitoring a cyber security issue and a cyber security incident and for protecting access to records of such activities;
d) contact information of employees who are designated to provide support when dealing with unexpected system or technical issues;
e) procedures for managing and approving of operational changes.

(3) The operational documentation includes, in particular:

a) *Operating Log Book*,
b) *Operation Control Inspection Plan*,
c) *Records of Operation Control Inspections*,
d) *Backup Plan*,
e) communication matrix in case of unexpected operational or technical problems,
f) special instructions for handling of outputs and media,
g) procedures for restart and recovery in the event of an IIS failure.

(4) The purchase of services necessary to ensure the operation of the IIS shall be carried out in accordance with the Act No. 134/2016 Coll. on Public Procurement and internal regulations issued by TBU, and shall be carried out exclusively in compliance with written contracts with clearly defined and measurable supply criteria.

Article 4
Safe operation requirements and standards

(1) All management documents in the field of operational security of information and communication technology are subject to a unified form of documentation management. The administrator of each document is in charge of the relevant documentation management. Administrators of individual documents are responsible for determining the validity period of the document, structure of the document, the employees and

departments/offices involved in the approval of the document, and the rules for handling of the document.

(2) Management documents in the sphere of ICT operational security are divided into three basic levels, depending on their area of competences:

a) Capacity management,
b) Technical vulnerability management,
c) Change management.

(3) The development and tests environments must be separate from the operation environment.

Article 5
Rules and restrictions for conducting cyber security audits and security tests

(1) Cyber security audits and security tests must always be carried out by a person qualified to perform such activities and also qualified to conduct an audit or test of technical equipment. The Cyber Security Auditor shall meet, at a minimum, the requirements set out in Annex 6 to the Decree on Cyber Security.

(2) The cyber security audit and security test must not impinge on the operation and the security of the audited IIS. All employees concerned providing operational support for the systems in question must be informed of the audit well in advance, and the CS Manager must give his/her consent to the audit.

(3) Cyber security audits and operational tests cannot be conducted while a security incident is occurring or when urgent measures are taken to mitigate the impact of technical vulnerabilities.

(4) The Cyber Security Auditor's accesses shall be monitored and logged, and all requirements, procedures and responsibilities shall be documented.

Document version			
Date	Version	Changed	Description of change
2 May 2024	01	CS Manager	Creation of document