Code:	SR/12/2024	
Reference number:	UTB/24/007645	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Organizational Security 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:	Information Technology Centre, Legal Services	
Pages:	6	
Appendices:	0	
Distribution list:	Employees of TBU in Zlín	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D., m. p.	

Article 1
Introductory provisions

(1) The Organizational Security Policy, as part of *the Declaration of Cyber Security of Tomas Bata University in Zlín*, sets out security roles and their responsibilities for the enforcement and implementation of security measures in compliance 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 with the Decree No. 82/2018 Coll., on Security Measures, cyber security incidents, reactive measures, requirements related to submissions in the field of cyber security and on data destruction (hereinafter referred to as the "Cyber Security Decree") in the context of Tomas Bata University in Zlín (hereinafter referred to as "TBU").

(2) With regard to the fact that TBU is the administrator and operator of important information systems (hereinafter referred to as the "IIS"), TBU must, in accordance with the Cyber Security Act, have the role of Cyber Security Manager (hereinafter referred to as "CS Manager") and of Primary/Supporting Asset Guarantor.

(3) The purpose of this policy is to define and describe the security roles that are part of the organizational structure of cyber security at TBU, and to determine the duties and responsibilities of a security role holder, to define the manner how security roles shall be determined and to describe mutual relations between the individual security roles.

(4) The individual terms used in this policy are defined, in particular, in the Cyber Security Act and in the Cyber Security Decree. An overview of the individual terms is included in the *Basic Concepts of Cyber Security* document, which is posted on the TBU website in the *Cyber Security* section.

Article 2
Security role holders, their rights and responsibilities

(1) The obligation to establish a Cyber Security Management Committee (hereinafter referred to as the "CS Committee") and the appointment of a CS Manager, the Cyber Security Architect (hereinafter the "CS Architect"), of Primary/Supporting Asset Guarantors and of the Cyber Security Auditor (hereinafter referred to as the "CS Auditor") is governed by the Cyber Security Act and by the Cyber Security Decree.

(2) Security roles are specified in detail in the relevant TBU internal regulations, in particular in the *Statute of the Cyber Security Management Committee,* in the *Statute of the Cyber Security Manager,* in the *Asset Management Policy* and in the confidential document entitled *Asset and Risk Assessment.*

(3) In the absence of an employee who holds a security role at a constituent part, the performance of this security role shall be taken over by an employee temporarily authorized to do so by the relevant superior.

I. Cyber Security Committee, its rights and responsibilities

(4) The CS Committee is responsible for activities related to the overall management and development of the IIS and is significantly involved in the management and coordination of activities related to the cyber security of information systems at TBU on the institutional level. Detailed information about competences, responsibilities and composition of the CS Committee are set out in the *Statute of the Cyber Security Management Committee*.

II. Cyber Security Manager, his/her rights and responsibilities

(5) The CS Manager is a security role holder responsible for planning, organizing and managing the implementation of measures, projects and programmes aimed to manage information security in such a manner as to achieve the objectives set out in the Cyber Security Act and in implementing regulations thereto, and that within the deadline set and within the budget approved. The CS Manager acts as a contact person for all aspects and issues of cyber security, who also promotes and coordinates the role of the Information Security Management System (hereinafter referred to as "ISMS") at TBU.

(6) The CS Manager is entitled to propose to the TBU Management organizational measures regulating the activities of, in general, an organizational, administrative or technical nature, including security aspects.

(7) The key activities, competences and responsibilities of the CS Manager are set out in the *Statute of the Cyber Security Manager*.

III. Primary Asset Guarantor, his/her rights and responsibilities

(8) Each primary asset must have its own Primary Asset Guarantor assigned.

(9) The Primary Asset Guarantor is responsible for assurance of the development, use, and security of the primary asset assigned (assurance of confidentiality, availability and integrity of the asset).

(10) The Primary Asset Guarantor

a) provides documents to the CS Manager for the purpose of conducting a risk analysis for the given primary asset,
b) in cooperation with the CS Manager, determines the value of the asset in terms of confidentiality, integrity and availability of the primary asset,
c) sets out general security requirements and concepts (e.g. required recovery times, access matrix related to the primary asset or other requirements for safe use, operation and development) for the primary asset based on classification,
d) following proposals from the CS Manager, from the Supporting Asset Guarantor or from the IT Administrator at a TBU component part, approves the proposed security rules and measures dealing with the security requirements concerning the given primary asset as well as concerning the related supporting asset such as an application service,
e) is responsible for the use, development and security of the asset;
f) informs the CS Manager of all changes to the asset which have or may affect the value of the asset.

IV. Supporting Asset Guarantor, his/her rights and responsibilities

(11) Each supporting asset must have its own Supporting Asset Guarantor assigned.

(12) The Supporting Asset Guarantor is responsible for assurance of the development, use and security of the supporting asset assigned (assurance of the confidentiality, availability and integrity of the asset).

(13) The Supporting Asset Guarantor:

a) assesses the confidentiality, integrity and availability of the supporting asset, and that based on the primary asset or on the superior technology layers of the supporting assets supported by the given asset,
b) ensures the implementation of security measures in accordance with security requirements and security documentation,
c) ensures the management of the supporting asset and is responsible for its use in accordance with security requirements and documentation, and in accordance with the assigned role,
d) informs the CS Manager of all changes to the asset that have or may have an impact on the value of the supporting asset,
e) informs the Guarantors of the relevant supporting assets about the superior technology layers.

V. IT Administrators at TBU component parts, their rights and responsibilities

(14) An IT Administrator at a TBU component part is an executive employee who, according to his/her job description, carries out at least one of the following activities:

a) Installation, configuration, administration, maintenance of HW/SW and records on HW/SW, including maintenance coordination,
b) Keeping of records on all computer equipment and means of communication entrusted to him/her,

c) Backing up of the system software and configurations, and protection of backup media,
d) Administration and registration of technical and security documentation prepared by him/her or entrusted to him/her,
e) Checking of audit records in compliance with security documentation,
f) Archival copies of audit records (logs).

(15) The IT Administrator at a TBU component part is responsible for managing, enforcing and checking of the security of information within the entrusted asset.

(16) The IT Administrator at a TBU component part maintains an up-to-date list of all authorized users including the access permissions assigned to them.

(17) The IT Administrator at a TBU component part sets the rules for data deletion and for disposal of technical data carriers in accordance with the Cyber Security Decree.

(18) The IT Administrator of the component part ensures that compliance with legal and licensing conditions is checked as regards the software used.

VI. IIS Administrator, his/her rights and responsibilities

(19) The IIS Administrator ensures the management, operation, use and security of the relevant technical asset.

(20) The IIS Administrator is responsible for the implementation of security measures during the operation of an IIS.

(21) At the same time, the IIS Administrator acts as the Guarantor of the relevant asset, carries out the instructions given by the senior executive in charge and by the Administrator of the primary asset.

Article 3
Requirements for the separation of activities of individual security roles

(1) The RACI matrix of cybersecurity security roles (see Table 1) depicts the links between role responsibilities and the individual ISMS areas. The letters R / A / C / I are used to depict the links.

a) R (Responsible) – The holder is responsible for direct implementation of the task entrusted to him/her.
b) A (Accountable) – The holder is responsible for ensuring that the process is carried out in accordance with the approved procedure.
c) C (Consulted) – The holder cooperates during the process.
d) I (Informed) – The holder is informed about the course and outcome of each stage of the process.

Field	**ROLES**					
	CS Committee	**CS Manager**	**Primary Asset Guarantor**	**Supporting Asset Guarantor**	**IT Administrator at a TBU component part**	**IIS Administrator**
Cyber security management	**A**	**R**	**R**	**R**	**R**	**R**
Cyber security audit	**I**	**C / I**	**C / I**	**C / I**	**C/ I**	**C / I**
Security measures proposed	**A**	**R**	**C**	**C**	**C**	**C**
Security measures implemented	**I**	**A**	**R**	**R**	**A**	**R**
Assurance of development, use, and security of a primary asset	**I**	**C**	**A**	**R**	**C**	**R**
Assurance of development, use, and security of a supporting asset	**I**	**C**	**C**	**A**	**C**	**R**

Table 1: RACI Matrix of Cybersecurity Security Roles

Article 4
Requirements for the separation of the performance of security and operational roles

(1) Due to conflicts of interest, the responsibilities and scope of competence related to the individual roles of the ISMS must be separated in such a manner as to reduce opportunities for misuse of assets or for their unauthorized or unintentional alteration.

(2) The roles of the CS Manager are not compatible with the roles responsible for the operation of the information and communication system and with other operational or managerial roles.

(3) The IT Administrator at a TBU component part must not be the IIS Administrator, Guarantor of the same primary asset, or the CS Manager.

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