Code:	SR/35/2023	
Ref. No.:	UTB/23/024491	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Declaration of Cyber Security at Tomas Bata University in Zlín	
Liability:	Tomas Bata University in Zlín	
Issue date:	8 November 2023	Version: 01
Effective from:	13 November 2023	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services	
Pages:	6	
Appendices:	0	
Distribution list:	TBU employees	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) The Declaration of Cyber Security at Tomas Bata University in Zlín (hereinafter referred to as the "Declaration") defines and specifies in detail the requirements for cyber security (hereinafter referred to as "CS") 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") in the environment of Tomas Bata University in Zlín (hereinafter referred to as "TBU").

(2) The purpose of this Directive is to declare and approve the basic security principles for the operation of important information systems (hereinafter referred to as "IIS") at TBU. The Declaration is a basic document for security policies and security documentation regulating CS at TBU.

(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
Liability

(1) The body or the person specified in § 3 of the Cyber Security Act is obliged to comply with the Cyber Security Act. This body or person shall cooperate and proceed at least to the extent set out in the Cyber Security Act. In accordance with the provisions of § 3 Letter e) of the Cyber Security Act, TBU is designated as the ISS administrator and operator.

(2) TBU, as the administrator and operator of the IIS, shall implement and apply security measures, report contact details, report cyber security incidents and shall implement measures as specified in the Cyber Security Act. The authority in charge of control is the National Cyber and Information Security Agency (hereinafter referred to as "NCISA").

(3) By issuing this Directive, TBU declares its interest in working towards a comprehensive solution to the issue of CS. The declaration has been prepared together with related security policies and security documentation.

(4) This Declaration is binding for all employees of TBU.

Article 3
Scope of competence

(1) In order to ensure and support CS, TBU shall adhere to this Directive, which:
   a) describes and explains the manners of securing IIS at TBU,
   b) describes the roles and competencies to ensure and perform the work tasks related to CS at TBU,
   c) specifies a security strategy,
   d) sets out the objectives and procedures of the security strategy,
   e) provides the structure of security policies and security documentation,
   f) includes information on the manner of revision of the Directive.

(2) The issue of CS concerns the entire structure of TBU in all its locations, including cooperating organizations that come into contact with the IIS of TBU.

(3) CS affects all identified assets of TBU, to the level and extent corresponding to the importance of the given asset.

Article 4
Roles and competencies

(1) The role of Cyber Security Manager (hereinafter referred to as the "CS Manager") and an advisory board - Committee for Cyber Security Management (hereinafter referred to as the "Committee for CS") have been established in order to ensure and perform the work tasks related to CS at TBU.

(2) The CS Manager shall ensure the actions resulting from the responsibilities of the Cyber Security Manager in accordance with the Cyber Security Act and the Decree on Cyber Security. All activities carried out by the CS Manager are described in the Rector's Directive - *Status of the Cyber Security Manager*.

(3) The Committee for Cyber Security Management has been established by the Rector of TBU in order to secure the management of CS at TBU in accordance with the Cyber Security Act and the Decree on Cyber Security. All activities carried out by the Committee for Cyber Security Management are described in the Rector's Directive - *Statute of Committee for Cyber Security Management.*

Article 5
Security strategies

(1) A security management strategy has been implemented for the purpose of securing the TBU IIS. The implementation of the security management strategy is based on the identification and assessment of risks of individual assets used for the operation of the IIS.

(2) According to the Cyber Security Act, the security management strategy is implemented through the following security measures:
   a) organizational measures,
   b) technological measures.

(3) According to the Cyber Security Act, organizational measures include the following:
   a) information security management system,
   b) risk management,
   c) security policy,
   d) organizational security,
   e) definition of security requirements on suppliers,
   f) asset management,
   g) human resources security,
   h) managing the operation and communications of critical information infrastructure and of an important information system,
   i) control of access of persons to critical information infrastructure or to an important information system,
   j) acquisition, development and maintenance of critical information infrastructure and of important information systems,
   k) managing cyber security issues and cyber security incidents,
   l) business continuity management,
   m) control and audit of critical information infrastructure and of important information systems.

(4) According to the Cyber Security Act, technological measures include the following:
   a) physical security,
   b) a tool for protecting the integrity of communication networks,
   c) a tool for verifying the identity of users,
   d) a tool for managing access rights,
   e) a tool to protect against malicious code,
   f) a tool for recording the activity of critical information infrastructure and important information systems, their users and administrators,
   g) a tool for detecting cyber security incidents,
   h) a tool for collecting and evaluating cyber security incidents,
   i) application security,
   j) cryptographic tools,
   k) a tool for ensuring the level of information availability,
   l) security of industrial and control systems.

Article 6
Objectives and procedures of the security strategy

(1) The aim of the security strategy is to ensure that CS is properly performed at TBU and that the operation of IIS is not restricted or disrupted in any manner through a breach of availability, confidentiality or integrity. Internal measures and procedures for fulfilling the basic objectives of the security strategy include prevention, detection and response at TBU.

(2) Prevention refers to preventive measures reducing the identified risks depending on their technical and economic feasibility. Risk analyses, including a draft Risk Management Plan, are prepared regularly once a year by the CS Manager, even in the event of substantial changes in the settings and configuration of the TBU IIS. Priority is given to the use of technical measures; organisational measures are chosen only if an equivalent technical measure does not exist or cannot be used under the given configuration or economic conditions.

(3) Detection consists of the implementation of organizational and technical measures to ensure timely detection of security issues and security incidents of TBU IIS. All systems must record important user activity, and functionality of their own SW and HW tools. An acceptable risk, which is not covered by relevant preventive measures, must be managed by a high-quality set of measures for the detection of security issues and incidents.

(4) Response refers to a specific procedure for the investigation, dealing with and, if necessary, renewal of the TBU IIS, primarily using organizational measures, with a use of technology to a certain degree.

(5) Procedures to ensure a security strategy include the following:
   a) ensuring compliance with legal regulations,
   b) ensuring uniform protection of the IIS according to the requirements of legislation,
   c) provision of adequate resources (personnel, technical and financial) for the area of CS,
   d) implementation of security technologies and their continuous updating and modernization,
   e) ensuring the ability to handle security issues and incidents,
   f) ensuring an adequate level of confidentiality, integrity and availability,
   g) formalization of processes and procedures,
   h) specification of responsibilities,
   i) increasing the level of security awareness of employees.

(6) TBU supports the objectives and procedures of the security strategy and considers the strategy of permanent provision of CS to be an integral part of its own management processes.

Article 7
Structure of documentation

(1) As part of the CS management, TBU maintains the following system of documentation:
   a) security policies,
   b) security documentation.

(2) Security policies are issued in the form of internal Rector's regulations to the following mandatory extent:
   a) Information Security Management System Policy,
   b) Asset Management Policy,
   c) Organizational Management Policy,
   d) Supplier Management Policy,
   e) Human Resources Security Policy,
   f) Communications and Operations Management Policy,
   g) Access Control Policy,
   h) Safe User Conduct Policy,
   i) Backup and Restore and Long-term Store Policy,
   j) Secure Information Transfer and Exchange Policy,
   k) Technical Vulnerability Management Policy,
   l) Mobile Device Security Policy,
   m) Acquisition, Development and Maintenance Policy,
   n) Privacy Policy,
   o) Physical Security Policy,
   p) Communication Network Security Policy,
   q) Malware Protection Policy,
   r) Policy of Deployment and Use of the Cyber Security Incident Detection Tool,
   s) Policy of Use and Maintenance of the Tool for the Collection and Assessment of Cyber Security Incidents,
   t) Policy of Safe Use of Cryptographic Protection,
   u) Change Management Policy,
   v) Cyber Security Incident Management Policy,
   w) Business Continuity Management Policy.

(3) Safety documentation shall be kept in the following mandatory scope:
   a) Cyber Security Audit Report,
   b) Report on the Review of Information Security Management System,
   c) Methodology for Asset Identification and Assessment and Risk Assessment,
   d) Asset and Risk Assessment Report,
   e) Statement of Applicability,
   f) Risk Management Plan,
   g) Security Awareness Development Plan,
   h) Record of Changes,
   i) Reported Contact Details,
   j) list of generally binding legal regulations, internal regulations and other regulations and contractual obligations.

Article 8
Revision

(1) The Declaration shall be reviewed at least once a year. The CS Manager is in charge of revising the document; and the final version of the document shall be approved by the Committee for CS. Even if there are no changes, the review date must be indicated for the version.

(2) The revision:

a) is focused on security policies and security documentation,
b) is aimed at ensuring compliance of technical and organizational measures with security policies and security documentation,
c) includes suggestion for improving CS at TBU,
d) includes proposals for changes in the IIS used at TBU.

Document version			
Date	Version	Changed	Description of change
30 October 2023	01	CS Manager	Creation of document