Code:	SR/40/2023	
Ref. No.:	UTB/23/025920	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Information Security Management System Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	27 November 2023	Version: 01
Effective from:	1 December 2023	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services	
Pages:	7	
Appendices:	0	
Distribution list:	TBU employees	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) The Information Security Management System Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* 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") at Tomas Bata University in Zlín (hereinafter referred to as "TBU").

(2) The purpose of this policy is to outline the strategic objectives of the Information Security Management System (hereinafter referred to as "ISMS"), the scope and limits of the ISMS and other rules and procedures related to the management of the ISMS.

(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
Objectives, principles and needs of information security management

(1) The aim of the ISMS is to ensure the security of information (in all its forms and processing phases) processed in the important information systems of TBU (hereinafter referred to as the "IIS") for the purpose of fulfilling its function as a public higher education institution.

(2) Information must not be available or disclosed to unauthorized individuals, entities or processes (the principle of confidentiality); they must be accurate and complete (principle of integrity) and must be accessible and usable at the request of an authorized entity (principle of availability).

(3) The following basic principles are taken into account when implementing the ISMS:

a) awareness of the need for information security management,
b) assigning responsibility for information security,
c) incorporating the commitment of the TBU management board to manage information security,
d) a risk assessment that determines the appropriate control mechanisms to achieve an acceptable level of risks,
e) incorporating security as a basic element of information networks and systems,
f) active prevention and detection of information security incidents,
g) ensuring a comprehensive approach to information security management,
h) continuous reassessment of information security and implementation of possible modifications.

(4) Information security management requirements are based on an assessment of assets and risks. As part of this process, threats, vulnerabilities and levels of individual risks are evaluated. Subsequently, appropriate corrective measures are defined.

(5) Through the Committee for Cyber Security (hereinafter referred to as the "Committee for CS") and the Cyber Security Manager (hereinafter referred to as the "CS Manager"), TBU must effectively reduce risks and the associated possible losses caused by breaches of confidentiality, integrity and availability of information, failure by TBU employees and damage to property.

Article 3
Scope and limits of the ISMS

(1) The scope and the limits of the ISMS are defined by the object parameter and the logical parameter. The ISMS does not apply to the information protection management system as specified in the Act No. 412/2005 Coll., on the Protection of Classified Information and Security Eligibility, as amended.

(2) The scope of the ISMS at TBU includes the following areas within the TBU IIS:

a) all acquired and processed information,
b) all related processes, human and material resources and relevant documentation,
c) personal data of TBU employees, TBU students, participants in TBU lifelong learning programmes, applicants for studies at TBU and TBU graduates,
d) TBU premises,
e) facilities and equipment owned by TBU,
f) information and communication infrastructure of TBU,
g) users of TBU IIS,
h) all suppliers (including subcontractors) who participate in the supply of primary and supporting assets also in terms of the services provided.

Article 4
Rules and procedures for documentation management

(1) Management of documentation and records at TBU is carried out using standard processes of the records management system, document administration and organizational rules. The CS Manager is responsible for managing the cyber security documentation and records process in cooperation with the Secretary to the Committee for CS.

(2) Security documentation:

a) consists of documents defined by the Cyber Security Act and the Decree on Cyber Security;
b) must be available to all persons performing activities in the area of CS at TBU;
c) is kept in the TBU records management system.

(3) When managing security documentation, procedures for the following activities are created, enforced and observed:

a) approving documents before they are issued and checking their correctness,
b) updating documents if necessary, including confirmation of their validity,
c) revision of documents at regular intervals, including confirmation of their validity,
d) marking changes and status after the last revision of documents,
e) prevention of unintentional use of outdated documents and their proper labelling if there is a need to keep the documents,
f) ensuring that up-to-date versions of documents are available,
g) ensuring legibility and easy identification of documents,
h) ensuring management, including distribution, proper labelling and separation of documents from other entities within activities carried out at TBU,
i) ensuring the principle of least privilege to documents (need to know).

Article 5
Rules and procedures for the management of resources and operation of an information security management system

(1) As part of the preparation of the CS management strategy, the demands on financial and human resources necessary to achieve the information security objectives set out in the ISMS shall be defined. The CS Manager shall present these requirements regarding the resources to the Committee for CS as part of the approval process. The Committee for CS is entitled to approve the CS strategy only if adequate financial and human resources are provided for its implementation.

(2) The resources for the development of technical aspects of CS are managed by the Bursar, while resources for the development of human resources, in particular for the education and training of users and experts, will be allocated in the relevant chapters of the budget with a fixed allocation for activities related to the development of information and cyber security.

(3) The use of financial resources allocated for the development of CS is subject to prior approval by the Committee for CS at TBU.

Article 6
Rules and procedures for conducting cyber security audits

(1) Independent audits of the state of CS, including compliance with legislative requirements in this area are carried out in accordance with § 16 of the Decree on Cyber Security at regular intervals at least every 3 years and in the event of significant changes.

(2) A CS audit must be carried out by a person who meets the conditions set out in § 7 Paragraph 4 of the Decree on Cyber Security, who shall independently assess whether the security measures are implemented correctly and effectively. CS audits are carried out by the Cyber Security Auditor (hereinafter referred to as the "CS Auditor"), who may be a TBU employee or an external entity – a legal entity or a natural person.

(3) Detailed planning and evaluation of the CS audit is the responsibility of the CS Manager and the Director of ITC and shall adhere to the Methodology for Conducting a Cyber Security Audit.

(4) The following activities take place as part of the CS audit:

a) controlling and keeping records of the observance of security policy, including the review of technical conformity;
b) assessment of the conformity between security measures and best practice, legal regulations, internal rules and regulations, other regulations and contractual obligations relating to the TBU IIS and imposition of possible corrective measures to ensure conformity.

(5) The CS audit report shall be submitted to the CS Manager and to the TBU management board.

(6) The results of the audit shall be taken into account in the Security Awareness Development Plan and Risk Management Plan.

Article 7
Rules and procedures for the review of the information security management system

(1) The ISMS is reviewed at least once a year, and in the event of significant changes in order to verify the purposefulness, effectiveness and adequacy of the implemented security measures operated by the ISMS in the form of an internal audit under the supervision of the CS Manager, or with the use of outsourcing in the form of an external service provided by a legal entity or a natural person.

(2) Inputs to the review of the ISMS include:
a) evaluated measures from the previous review of the ISMS,
b) identified changes and circumstances that may affect the ISMS,
c) feedback on the performance of the ISMS, in particular:

- non-conformance and corrective measures,
- monitoring and measurement results,
- results of previous CS audits,
- fulfilment of the objectives of the ISMS,

d) results of the risk assessment and status of implementation of the risk management plan,
e) outputs of vulnerability scanning and penetration testing,
f) list of cyber security occurrences and cyber security incidents in the past period,
g) evaluation of the CS educational plan.

(3) Outputs of the review include:
a) identification of opportunities for continuous improvement;
b) recommending necessary decisions, determining corrective measures and persons performing individual activities.

(4) The CS Manager shall prepare a report from the review of the ISMS, which shall be approved by the Committee for CS and later submitted to the TBU management board.

Article 8
Assessment of the quality of the security management process

(1) Metrics that indicate the quality of security management process include:

a) the frequency and extent of cyber security occurrences and incidents that resulted in a breach of the confidentiality or integrity of the information processed in the TBU IIS,
b) the frequency and extent of cyber security occurrences and incidents that resulted in a breach of the availability of information,
c) the frequency and the number of cases of damage to TBU's prestige or good reputation,
d) the frequency and the extent of breaches of security policy,
e) the presence of a security concept as part of every step and decision in the development of the TBU IIS,
f) general awareness of the principles of security and specific knowledge of the security policy among competent employees and their perception of the need to ensure security.

Article 9
Rules and procedures for corrective measures/actions and improving the ISMS

(1) The ISMS shall be continuously monitored through established procedures and means (in accordance with Articles 5 and 6). The ISMS shall be also maintained and improved through the non-conformance and incident management system.

(2) All corrective measures/actions shall be based on the ISMS review report. Corrective measures shall be discussed by the Committee for CS; persons in charge of the implementation of corrective measures and responsible for complying with the deadline for the implementation of the corrective measures shall be appointed for each corrective measure.

(3) Corrective measures for non-conformities and incidents arisen shall be proposed and implemented by the CS Manager in cooperation with the Director of ITC. As part of a proactive approach, the CS Manager shall also implement preventive measures to improve the ISMS.

(4) Corrective measures are monitored semi-annually at meetings of the Committee for CS.

Article 10
Classification and access to information

(1) The classification of information is a tool for ensuring the adequacy of protection of the information assets of TBU. Information is distributed and requirements for its protection are set in accordance with the established rules. The classification of information provides users with information about the need for special handling of information.

(2) The classification of information and the security measures corresponding to it must take into account the needs of TBU regarding the sharing of information or the restriction of access to it, and above all the level of potential negative impacts in the event of a breach of the information security policy.

(3) Information and outputs from systems that process classified information must be labelled in accordance with their value and sensitivity.

(4) When information is created, or when receiving information from third parties, the employee who has received the information shall decide whether the information requires special protection based on an assessment of the criticality of the information.

(5) The classification scheme for access to information comprises these levels of information classification:

a) **Public** – information that is accessible to all TBU employees, TBU students and the general public and is approved by the owner for publication. The information does not require a special level of protection in terms of confidentiality. However, it is necessary to pay attention to the protection of the information from the point of view of integrity, so as not to publish information that does not correspond to reality. Access to public information must not be restricted.
b) **Internal** – information that is intended for internal use by all TBU employees, TBU students or a selected group, however, not through publicly available channels. The information may be shared within the recipient's organization and/or also with other partner entities of the recipient that are bound by appropriate confidentiality agreements and need this information to fulfil contractual obligations. At the time of the transmission, the recipient must set the level of confidentiality of the communication to ensure an adequate degree of protection during transmission and storage.
c) **Confidential** – the information is not publicly available and the protection thereof is required by legal regulations, other regulations or contractual arrangements. The information may not be disclosed to any person other than the person for whom such information was intended, unless other persons to whom such information may be provided are explicitly specified.

Document version			
Date	Version	Changed	Description of change
27 November 2023	01	CS Manager	Creation of document