Code:	SR/7/2023	
Category:	RECTOR'S DIRECTIVE	
Reference number:	UTB/23/005941	
Type of document:	INTERNAL	
Title:	Status of the Cyber Security Manager	
Liability:	Tomas Bata University in Zlín	
Issue date:	30 March 2023	Version: 01
Effective from:	3 April 2023	
Issued by:	Rector	
Prepared by:	Information Technology Centre	
In cooperation with:	Legal Services	
Pages:	5	
Appendices:	0	
Distribution list:	All TBU employees	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D., m.p.	

Article 1
Introductory provisions

(1) The Cyber Security Manager (hereinafter referred to as the "CS Manager"; cyber security hereinafter referred to as "CS") at Tomas Bata University in Zlín (hereinafter referred to as "TBU") ensures the tasks arising from the duties to be accomplished as part of the job position of the Cyber Security Manager in compliance with Act No. 181/2014 Coll., on Cyber Security and on Amendments to Related Acts (Cyber Security Act), 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 Set for Complaints Related to Cyber Security and Data Destruction (hereinafter referred to as the "Decree on Cyber Security").

(2) The job position of the CS Manager at TBU may be occupied by a TBU employee or provided through an external entity – a natural person or a legal entity.

(3) The CS Manager is subordinate to the TBU Rector and, during the performance of his/her job, he/she shall follow instructions given by the TBU Rector in accordance with requirements set in legal regulations and internal regulations in TBU conditions.

(4) The CS Manager is authorized to communicate with regulatory authorities in the field of cyber and information security, in particular with the NÚKIB and the GovCERT.CZ/CSIRT. CZ.

Article 2
Basic terms

Assets

Primary assets include information or services that are processed or provided by an information and communication system.

Supporting assets include technical assets, employees and suppliers involved in the operation, development, management or security of an information and communication system.

Technical assets include the hardware, means of communication and software of an information and communication system as well as facilities where these systems are located and whose failure may have an impact on the information and communication system.

The guarantor of the primary asset is, most often, an employee holding a job position such as Head of Department, Head of Section, process owner, system owner, etc.

The guarantor of the supporting asset shall be selected depending on his/her job position, procedural and specialized knowledge of the given asset. He/she must be able to assess the asset as regards its possible impacts so that the person responsible for carrying out the risk assessment is able to adequately assess and manage such risks.

Security teams play a key role in protecting the critical information infrastructure and important information systems in compliance with the Cyber Security Act and with its implementing regulations. Another task of such teams is also to act as the primary source of security information and assistance for state authorities, organizations and citizens.

GovCERT.CZ is a government team of the National Cyber Security Centre; its main activities include dealing with security incidents, in particular through consulting and provision of network data analysis and log analysis services with the aim of identifying the manner and consequences of an incident.

CSIRT is a universal abbreviation for the Computer Security Incident Response Team.

CSIRT. CZ is the national CSIRT team of the Czech Republic, which is operated by the CZ.NIC association in accordance with the Cyber Security Act and with a public contract concluded with the National Security Authority.

The National Cyber and Information Security Agency (hereinafter referred to as "NÚKIB") is the central administrative authority for cyber security, including the protection of confidential information in the field of information and communication systems and cryptographic protection.

The Information Security Management System (hereinafter referred to as "ISMS") is a documented system where defined information assets are protected, information security risks are managed, and the implemented measures are checked. When implemented in an organization, the procedure shall adhere to the international standard ISO/IEC 27001.

An update refers to a system update that modifies or improves the existing version. Updates are made in order to implement higher security or fix bugs.

An upgrade refers to the replacement of the current version of a system with a new or higher version.

Article 3
Rights and responsibilities of the CS Manager

(1) The CS Manager is responsible for ensuring and managing the implementation of cyber and

information security projects and programmes approved by the Committee for CS in compliance with instructions given by the TBU Rector, and that in a manner enabling that TBU's information and communication infrastructure provides services in this area in accordance with the current legislation applicable to the field of cyber and information security.

(2) The CS Manager is responsible for creating, enforcing and ensuring the ISMS, from research and analyses through continuous testing of prevention up to the elimination of consequences and assessment of cyber incidents at TBU.

(3) The CS Manager is responsible for creating internal regulations as well as for enforcing and ensuring that internal regulations related to the CS topic are updated.

(4) The CS Manager cooperates during the identification of the current scope and completeness of information on assets, identification of sources, and during the process of proposing of ways and means to be used to add the missing information.

(5) The CS Manager is responsible for ensuring TBU's ability to implement security measures (organizational and technical) imposed by the Cyber Security Act and for a timely and economical implementation of such measures.

(6) The CS Manager shall continuously analyse the development of the ISMS and assess the cyber risks identified, the cyber security events detected and the cyber incidents detected; he/she shall submit a report on the above to the Committee for CS. The report shall also include proposals or mitigation of unacceptable risks and proposals for changing the priorities of security projects, and that regularly every six months.

(7) The CS Manager is entitled to determine:

a) the scope and limitation of the ISMS (with regard to assets and organizational security), where the CS Manager shall determine which organizational parts and technical elements are covered by the ISMS,
b) a unified methodology for identification and assessment of assets and a methodology for setting of criteria related to risk acceptability,
c) aims of continuity of activities and a strategy (plan) for management of continuity of the following activity, including the standardization of cyber and information security processes,
d) operational rules and procedures for the ISMS,
e) A Risk Management Plan listing the aims and benefits of the security measures adopted for risk management, including the designation of the person authorized to ensure the implementation of security measures.

(8) The CS Manager cooperates during the approval process of binding regulations applicable to the selection, unification and systemization of technical and software tools of information technology in TBU conditions.

(9) In the case of projects related to information systems, usually when implementing a new system or when updating/upgrading a system already in operation, the CS Manager shall:

a) discuss the organization of inspections of stages of specific performance types,

b) decide, in cooperation with the system integrator, on the preparation of test data and on the organization of security testing,
c) be informed about the test and verification operation and stress tests,
d) participate in the preparation and organization of the acceptance procedure.

(10) The CS Manager checks the formulation of the terms and conditions of public tenders as regards the factual aspect (including small-scale public tenders) for the construction and modernization of TBU's information and communication systems or for the acquisition of supplies or services whose components may affect CS at TBU in terms of cyber security standards and provides assistance to the contracting authority in tender procedures related to dealing with CS-related issues; a more detailed regulation may be specified in separate TBU internal rules.

(11) The CS Manager cooperates during the process of managing of risks, of the risks' scope and impact.

(12) The CS Manager coordinates the management of cyber incidents.

(13) The CS Manager decides on the implementation of a security measure depending on the information provided by monitoring and surveillance systems, on opinions given by the Committee for CS or on decisions taken by the NÚKIB.

(14) The CS Manager provides/is in charge of:

a) detection of cyber security events,
b) preparation of Asset and Risk Assessment Reports, Risk Management Plan and Applicability Statement, to be submitted to the Committee for CS,
c) regular risk assessment related to suppliers, performing of checks on the implemented security measures concerning the services provided and remedy of the identified deficiencies,
d) updates to the ISMS and to the relevant documentation according to the results of audits or significant changes and assessment of suitability and effectiveness of security measures,
e) updates to the Asset and Risk Assessment Report, the Security Policy, the Risk Management Plan and the Security Awareness Development Plan,
f) preparation of supporting documents for the implementation of reactive measures issued by the NÚKIB and for the implementation of security measures (organizational and technical),
g) cooperation during the CS control audits carried out by NÚKIB and during their analysis.

(15) The CS Manager shall prepare a Security Awareness Development Plan and inform the Committee for CS of this Plan.

(16) The CS Manager coordinates measures aimed to increase security awareness in TBU conditions, including staff training on cyber and information security.

(17) The CS Manager supervises the establishment of rules for suppliers (provision of instructions aimed to assure information security during the creation, assessment, selection, management and termination of supplier relationships in the field of information

and communication technologies) from the perspective of meeting the requirements set in the Cyber Security Act and in the implementing regulations.

(18) The CS Manager shall regularly report to the TBU management board on the current state of the ISMS, on security incidents, on identified non-conformities and on insufficient effectiveness of security measures.

(19) The CS Manager regularly communicates with the TBU management board.

Article 4
Competences of the CS Manager

(1) The CS Manager is entitled to request that the Committee for CS should issue statements and express opinions on:

a) the acceptability/unacceptability of identified cyber security risks, including the determination of a still acceptable level of risk and the setting of a limit of funding to be used for elimination of unacceptable risks,
b) priorities for the implementation of security measures and of the security projects proposed,
c) designation of persons authorized to perform the roles of asset guarantors,
d) implementation of basic identification of assets.

(2) The CS Manager is entitled to request that the guarantors of primary assets should process and submit:

a) information on the purpose of the system and on the conditions of its operation,
b) identified primary assets and their risks,
c) assessment of the acceptability of such risks by setting the security parameters (levels) of services provided by the system.

(3) The CS Manager is entitled to request that the guarantors of supporting assets and administrators should do the following:

a) identify supporting assets and their risks,
b) assess the acceptability of such risks, including the possibility of risk transfer,
c) assess the efficiency of cyber security measures.

Version of document			
Date	Version	Changed	Description
30/03/2023	01	CSM Status	Creation of document