Code:	SR/14/2026	
Ref. No.:	UTB/26/012224	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Cyber Security Incident Management Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	23 February 2026	Version: 01
Effective from:	27 February 2026	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services	
Pages:	3	
Appendices:	0	
Distribution list:	TBU employees	
Signature of authorised person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) The Cyber Security Incident Management Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* sets out procedures and responsibilities for individuals in cases of cyber security incidents and elaborates on cyber security requirements in accordance with Act No. 264/2025 Coll., on Cyber Security (hereinafter referred to as the "Cyber Security Act") and related legal regulations at Tomas Bata University in Zlín (hereinafter referred to as "TBU").

(2) The purpose of the policy is to establish procedures to reduce the impact of cyber security incidents, stop their spread, and prevent their recurrence.

(3) This policy applies to all users and information assets. 'Users' shall mean students, employees engaged under an employment contract or agreement (hereinafter referred to as "TBU employees"), emeritus professors, and scholarship holders engaged under cooperation agreements; and, as appropriate, employees of third parties who may, under predefined conditions, enter the protected premises of TBU.

(4) The individual terms used in this Directive are defined particularly by the Cyber Security Act and related legal regulations. 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
Definition of categories of cyber security incidents

(1) Cyber security incident categories are determined by their severity and expected impact on TBU assets:

a) Category "I" – a less serious incident involving a minor breach of the security of services or assets provided. Its resolution requires the intervention by asset guarantors or administrators to limit the further spread of the incident, including the minimisation of any damage incurred.
b) Category "II" – a serious incident in which the security of the services or assets provided is compromised. Its resolution requires immediate intervention by asset guarantors or administrators to prevent further spread of the incident, including the minimisation of any damage incurred.
c) Category "III" – a very serious incident in which the security of the services or assets provided is directly and significantly compromised. Its resolution requires immediate intervention by asset guarantors or administrators to prevent further spread of the incident, including the minimisation of both incurred and potential damage.

(2) If it is not an incident referred to in Paragraph 1, it is a cyber security event.

Article 3
Rules and procedures for identifying, recording, and managing individual categories of cyber security incidents

(1) A tool for detecting cyber security incidents has been implemented at TBU.

(2) TBU has designated a tool for recording, managing, and resolving operational and security events and incidents, which serves as a single point of contact.

(3) TBU has established procedures and roles for analysing cyber security events, categorising them, and assessing whether they constitute a cyber security incident.

(4) Procedures for managing cyber security incidents are established in accordance with the asset and risk assessment of individual elements of information and communication technologies.

(5) As part of the classification of cyber security incidents, the impacts, the need for response, and the urgency of resolution are assessed.

(6) The form and requirements for reporting cyber security incidents to the National Cyber and Information Security Agency (hereinafter also referred to as "NCISA") are set out in the Decree on Cyber Security.

(7) The Cyber Security Manager at TBU is responsible for reporting cyber security incidents to the NCISA.

Article 4
Rules and procedures for testing the cyber security incident management system

(1) The testing of the cyber security incident management system shall be documented and controlled.

(2) The testing of the cyber security incident management system shall be conducted once a year.

(3) Only test data is used to test the cyber security incident management system.

Article 5
Rules and procedures for evaluating cyber security incidents and improving cyber security

(1) Each cyber security incident is evaluated in terms of its impact on the confidentiality, availability, and integrity of individual assets.

(2) The results of the cyber security incident evaluation serve as a basis for improving cyber security.

(3) Measures resulting from the evaluation of a cyber security incident serve as input for updating the Risk Management Plan.

(4) Each cyber security incident, its evaluation, including proposed measures, shall be submitted to the Cyber Security Committee for discussion.

Article 6
Reporting and recording of events and incidents

(1) The recording of cyber security events and incidents at TBU is centrally managed in a tool designated for recording, managing, and resolving operational and security events and incidents.

(2) In the event of a suspected or detected cyber security event or incident, the user is required to proceed in accordance with the information provided on the TBU website in the *Cyber Security* section, specifically on the *Cyber Incident Reporting* website – https://www.utb.cz/en/university/about-the-university/structure/advisory-boards/committee-for-cyber-security-management/cyber-incident-reporting/.

(3) The Director of the Information Technology Centre is responsible for maintaining records of cyber security events and incidents.

Document version			
Date	Version	Changed	Description of change
23 February 2026	01	CS Manager	Creation of document

This English version of the internal regulation is not legally binding; it is for informational purposes only and does not have to correspond to the Czech version of the original document.