Code:	SR/10/2026	
Ref. No.:	UTB/26009917	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Business Continuity Management Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	16 February 2026	Version: 01
Effective from:	20 February 2026	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services	
Pages:	4	
Appendices:	0	
Distribution list:	Tomas Bata University in Zlín	
Signature of authorised person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) The Business Continuity Management Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* lays down rules for minimising losses caused by potential accidents (fire, gas explosion, interruption of electricity supply, loss of computing capacity or communication channels, unavailability of external services, terrorist attack, etc.) or natural events (e.g., flooding, torrential rain, lightning strike, wind storms), and further elaborates the requirements for cybersecurity in accordance with the 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 this Policy is to:

a) define the rights and responsibilities of the persons concerned;
b) establish business continuity management objectives with regard to the minimum level of services provided, the information system recovery time objective (RTO) and the data recovery point objective (RPO);
c) set out methods for assessing the impact of cyber security incidents on continuity and for evaluating the related risks;
d) specify the content of business continuity plans and disaster recovery plans for individual information systems;
e) establish and implement procedures for carrying out measures issued by the National Cyber and Information Security Agency (hereinafter also referred to as "NCISA").

(3) This Policy is binding on employees of TBU who, within the scope of their responsibilities, participate in the administration and operation of TBU information systems.

(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
Rights and obligations of the persons concerned

(1) 'Persons concerned' shall mean security roles as defined in the *Organisational Security Policy* and users of information systems.

(2) The rights and obligations of the persons concerned in the area of cybersecurity arise from the information security management system specified by the *Information Security Management System Policy* and other internal regulations of TBU.

(3) The exercise of the rights and obligations of the persons concerned is conditioned by the structure of resources, the setting of procedures and activities within the administration and operation of TBU information and communication technology components.

Article 3
Objectives of business continuity management

(1) The objectives of business continuity management are to:

a) determine, on the basis of the outputs of risk assessment and business impact analysis, the minimum scope of services provided by individual functional areas of important information systems (hereinafter also referred to as "IIS") of TBU;
b) ensure the security and continuity of information and communication technology services even in the event of a cyber security event or incident, emergency, or disruption to information and communication technology services;
c) initiate steps to restore services to the required level;
d) minimise damage to property or assets of the IIS of TBU arising as a result of a major incident.

(2) Business continuity processes shall be managed and documented.

(3) Each primary asset shall have a defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Minimum service level

(4) The minimum service level refers to the minimum scope of information and communication technology services for the use, operation, and administration of the IIS.

Recovery time objective

(5) The Recovery Time Objective (RTO) shall mean the period within which information and communication technology components are restored to the defined service level.

Recovery point objective

(6) The Recovery Point Objective (RPO) shall mean the point in time to which data are restored in order to achieve the relevant service level.

(7) The full data recovery point shall mean the point in time at which data are fully restored.

Article 4
Business continuity management policy for achieving continuity objectives

(1) To achieve continuity objectives, Asset Guarantors shall develop, manage, and regularly update business continuity plans and disaster recovery plans for information and communication technology components and related services.

(2) Business continuity plans and disaster recovery plans shall be tested regularly.

Article 5
Methods for assessing the impact of cyber security incidents on continuity and evaluating related risks

(1) The assessment of the impact of a cyber security incident on continuity and the evaluation of related risks shall form part of the business impact analysis conducted within the assessment of primary assets and their dependencies on supporting assets. When determining asset value and associated risks, due consideration shall also be given to the impact on ensuring the continuity of the relevant asset.

Article 6
Determination and content of required business continuity and disaster recovery plans

(1) For each IS, the business continuity plan and the disaster recovery plan shall be incorporated into a single document.

(2) This document shall in particular include:

a) asset valuation and the determination of impacts and risks related to threats to business continuity;
b) the minimum service level;
c) the recovery time objective for achieving the minimum service level;
d) the data recovery point objective for achieving the minimum service level;
e) the recovery time objective for achieving the full service level;
f) the data recovery point objective for achieving the full service level;
g) a description of dependencies between individual components of information and communication technologies;
h) the financial, technical, human and information resources necessary for implementation;
i) rules for updates and testing plans;

j) measures implemented to prevent the occurrence of a cyber security event or incident;
k) procedures to be followed in the event of a cyber security event or incident, or major incident;
l) the responsibilities of the individual persons concerned,
m) the sequence and timing of activities,
n) linkages to disaster recovery plans of other information systems.

Article 7
Procedures for the implementation of measures issued by NCISA

The implementation of measures issued by the NCISA shall be governed by the rules set out in this Policy.

Document version			
Date	Version	Changed	Description of change
16 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.