Code:	SR/37/2024	
Ref. No.:	UTB/24/026134	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Backup and Recovery and Long-Term Retention Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	29 October 2024	Version: 01
Effective from:	1 November 2024	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services, Data Protection Officer	
Pages:	4	
Appendices:	0	
Distribution list:	TBU employees	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) The Backup and Recovery and Long-Term Retention Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* defines security roles and their responsibilities for enforcing and implementing of security measures 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 define the principles and processes of data backup within important information systems (hereinafter referred to as the "IIS") 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
Backup and recovery requirements

(1) The Cyber Security Manager (hereinafter referred to as the "CS Manager"), in cooperation with the TBU Information Technology Centre (hereinafter referred to as the "ITC"), shall determine the backup requirements for each primary asset. The minimum backup and recovery requirements are as follows:

a) the extent of the backup;

b) the Recovery Time Objective (hereinafter referred to as the "RTO"), which refers to the time at which the affected information assets reach the specified level of services;
c) the Recovery Point Objective (hereinafter referred to as the "RPO"), which refers to the point at which data is recovered.

(2) Backup requirements shall be implemented by the Primary Asset Guarantor in at least the following areas:

a) preparation of the *Backup Plan*,
b) management of backup capacities,
c) performing of backups and restores and updating of the *Backup Plan*,
d) control of backups,
e) recovery test.

Article 3
Backup rules and procedures

(1) Each element of the primary asset shall have a *Backup Plan*. The Backup Plan shall be a confidential document with restricted access, prepared by the Primary Asset Guarantor, and shall contain at least the following information:

a) the extent of the backup,
b) specification of the RTO and the RPO,
c) the expected volume of data to be backed up,
d) specification of the backup method,
e) retention period for the backups,
f) a description of the backup creation process,
g) specification of the backup medium and the method of storage,
h) security of backups and media,
i) specification of the method and extent of the tests of data recovery from backups.

(2) The backup process is monitored. The Primary Asset Guarantor is responsible for the success of the backup process.

Article 4
Rules and procedures for long-term storage

(1) Backups for long-term storage shall be deposited:

a) outside the device of the backed-up IIS,
b) outside the primary IIS data storage facility.

(2) The backup carriers shall be labelled and recorded.

(3) Long-term backup storage facilities shall comply with physical security and personal data protection rules.

(4) Access to backup storage areas shall be controlled by and restricted to authorized persons only.

Article 5
Rules for secure backup and long-term storage of information

(1) At least the following information shall be specified regarding the long-term storage:
   a) the duration of the storage of information, including archiving,
   b) the method of access to archived data,
   c) the method of disposal of the data.

(2) Long-term storage of information and backup media shall be provided by the Primary Asset Guarantor in cooperation with the ITC.

(3) The rules for secure backup and long-term storage of information are set out in the *Backup Plan*.

(4) Information shall be stored in accordance with the applicable legislation that determines the period of its retention and in accordance with the *TBU Regulations for Document Filing and Shredding*, as amended. In the case of backup and storage of information containing personal data, it is necessary to proceed in accordance with the approved *Personal Data Processing Record* held in the TBU Purpose Register.

Article 6
Recovery rules and procedures

(1) Recovery procedures shall include a description of the recovery process and shall form part of the *Backup Plan*.

(2) Recovery rules shall specify at least:

   a) the extent of the recovery,
   b) the source of the recovery,
   c) the target of the recovery,
   d) the recovery test.

Article 7
Backup and recovery testing rules and procedures

(1) Verification of the readability, completeness and recoverability of data from backups is part of the *Backup Plan* and shall be performed periodically as specified in the *Backup Plan*.

(2) The performance of the tests of data recovery from backups shall be documented.

(3) The performance of data recovery tests shall not adversely affect the operation of the IIS.

(4) Corrective action shall be taken if errors are detected during the test.

Article 8
Policy on access to backups and stored information

(1) Only those persons performing the backup shall have access to the backup media. Other persons may gain access to the backup media, if reasonably necessary, with the written permission of the CS Manager.

Document version			
Date	Version	Changed	Description of change
29 October 2024	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 document.