

Code:	SR/1/2025	
Ref. No.:	UTB/25/000183	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Technical Vulnerability Management Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	8 January 2025	Version: 01
Effective from:	13 January 2025	
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 Technical Vulnerability Management Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* sets out procedures and protocols supporting effective asset management 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 identify vulnerabilities that could limit the functionality or security of the operation (hereinafter referred to as “technical vulnerabilities”) of an important information system (hereinafter referred to as the “IIS”), to determine how to take measures to address and eliminate the vulnerabilities, to establish rules for limiting the installation of software, to establish rules and procedures governing the search for patch software packages, to establish rules and procedures governing the testing of software patches, and to establish rules and procedures governing the deployment of software patches at TBU.
- (3) This policy shall apply to all TBU staff, to information assets created or used within the IIS, and to users of those assets.
- (4) 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

Technical vulnerabilities in assets

- (1) To determine technical vulnerabilities, assets refer to all primary assets and selected supporting assets in the software category according to the catalogue of primary and supporting assets in the confidential document *Asset and Risk Assessment*.
- (2) The technical vulnerabilities in assets referred to in Paragraph 1 are divided into:
 - a) bugs in the programming code that have arisen during the development of products or during updates and patches to products,
 - b) errors in the installation and configuration of technical assets and installed software.
- (3) The software vulnerability management process is documented and based on:
 - a) identification of vulnerabilities,
 - b) prioritisation of vulnerability solutions,
 - c) addressing of vulnerabilities in order of priority,
 - d) implementing a workaround when a fix is not available,
 - e) control of the measures applied.
- (4) A methodology shall be developed to remove the technical vulnerabilities of the assets referred to in Paragraph 1, including at least the identification of the source of the fix, the method of testing and the deployment plan.

Article 3

Restriction rules for software installation

- (1) The catalogue of primary and supporting assets in the confidential document *Asset and Risk Assessment* shall contain at least the following information for software:
 - a) the supplier and manufacturer of the software,
 - b) the current version in use,
 - c) the location of the software.
- (2) Only such software may be installed as is necessary for its proper functioning and administration and as is recommended by the supplier of such software.
- (3) It is forbidden to install unapproved software, versions of software with known vulnerabilities or security threats reported by superior organizations (e.g. the National Cyber and Information Security Agency) and the CESNET organization, interest associations of legal entities established in accordance with the Civil Code by public higher education institutions in the Czech Republic and the Academy of Sciences of the Czech Republic.
- (4) The installation of new software is subject to a process of recording and monitoring changes, and the guarantor of the relevant asset is responsible for the proper installation of the software.

Article 4

Rules and procedures governing the search for patch packages

- (1) The guarantor of the relevant asset shall regularly monitor information about technical vulnerabilities from available sources, identify risks and propose methods of resolution to the Director of the Information Technology Centre of TBU (hereinafter referred to as “ITC”).
- (2) The Director of ITC, together with the relevant guarantors, shall assess the risks and determine the course of action.
- (3) Following approval by the Director of ITC, the guarantor of the relevant asset shall ensure that the patch software packages are installed.
- (4) The Director of ITC shall inform the CS Manager of the procedure under Paragraphs 1 to 3.

Article 5

Software patch testing rules and procedures

- (1) Testing of patches and new software shall be performed in an environment separate from the production environment.
- (2) The tests must demonstrate the correctness of the software modifications.
- (3) Deployment into the production environment shall be made after successful evaluation of the tests and approval by the guarantor of the relevant asset.
- (4) If software testing cannot be performed due to increased costs or lack of resources, all risks associated with deploying software repairs shall be evaluated.

Article 6

Software patch deployment rules and procedures

- (1) For each asset, the software patch deployment process shall be managed and documented in accordance with *Annex 1b Asset Management Policy – Asset Handling*.
- (2) As part of the deployment of software patches into the production environment, Recovery Point Objectives and data backups shall be established.
- (3) When deploying software patches, previous versions of the software shall be backed up.
- (4) If a patch for an identified vulnerability is not available or the side effects of its use are unacceptable, the guarantor of the relevant asset shall take alternative control measures, such as:
 - a) shutting down the services affected by the vulnerability,
 - b) modifying firewall settings or other user access control measures,

- c) increasing user awareness of how to detect and respond to attacks; or
 - d) increased monitoring of activity to detect attacks against the vulnerability.
- (5) In certain exceptional circumstances where the confidentiality, availability and integrity of data could be immediately compromised, the guarantor of the relevant asset shall allow a patch to be installed in accordance with the cyber security incident response process, rather than the change management process. Any such decision, which must be approved by the Director of the ITC, shall be recorded by the guarantor of the relevant asset and reported to the CS Manager and the Data Protection Officer.

Document version			
Date	Version	Changed	Description of change
8 January 2025	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.