Code:	SR/15/2025	
Ref. No.:	UTB/25/023381	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Acquisition, Development, and Maintenance Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	15 May 2025	Version: 01
Effective from:	19 May 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 Acquisition, Development, and Maintenance Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* sets out the security requirements for changes to an important information system (hereinafter referred to as "IIS") 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 ensure information security in the acquisition, development and maintenance of the IIS, to establish rules and procedures for the acquisition, development and maintenance of software, including recordkeeping, and to establish rules and procedures for monitoring compliance with license terms.

(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
Security requirements for acquisition, development and maintenance

(1) Security requirements must be incorporated already at the stage of system selection and design. They must be documented by the primary asset guarantors and included in contracts with IIS suppliers.

(2) Security requirements must be defined and implemented based on the classification of the primary assets of the given system and the results of a risk analysis.

(3) For each new system, acceptance criteria must be established, covering both functional and security requirements. These criteria must be evaluated as part of the acquisition process and before the new system is put into productive operation.

(4) During development, the security of the development and testing environments must be ensured, including their separation from the production environment.

(5) The transition of a new system into the production environment, as well as the maintenance of all systems, must be carried out in accordance with change management procedures.

(6) Version control of software must be maintained throughout the entire system lifecycle, including the ability to revert to a previous version if necessary.

(7) Operational, design, user and security documentation shall be kept up to date throughout the entire development process.

(8) The acquisition and development process shall be planned, documented, and managed by the IIS suppliers.

(9) The primary asset guarantor shall:
   a) collaborate in defining the functional requirements for the acquisition and development of IIS,
   b) ensure the classification of the asset,
   c) establish access control rules for the asset,
   d) and define maintenance requirements for IIS in cooperation with the Information Technology Centre.

(10) The asset lifecycle and acquisition process include security requirements and security measures based on the applicable security policy, identified risks, and the requirements of the primary asset guarantors.

(11) The development, changes and maintenance of assets are carried out in accordance with the established process, which takes into account principles of safe development and change management, testing within a separate environment, code review, and where applicable, independent third-party security audits.

Article 3
Vulnerability management

(1) The asset vulnerability management process is planned, documented and managed by the IIS suppliers. It is based on:
   a) identifying vulnerabilities,
   b) addressing vulnerabilities according to priority,
   c) monitoring the implementation of corrective measures.

(2) Technical review of applications after changes to the IIS technical and software configuration requires at least:

a) identifying vulnerabilities,
b) establishing priorities for addressing vulnerabilities,
c) addressing vulnerabilities according to priority,
d) monitoring the implementation of corrective measures.

(3) Changes to software are limited to necessary modifications and are all managed. If it is necessary to adjust the software, the following aspects are considered:
a) risks of the proposed measures and processes ensuring integrity,
b) compliance with licencing policies,
c) collaboration with suppliers during software updates,
d) compatibility with other used software.

Article 4
Software and information licensing and acquisition policy

(1) Only authorized software with a valid license or authorized software for which no license purchase is required by the author or supplier, shall be installed on all devices operated by TBU.

I Rules and procedures for software deployment and its registration

(2) The primary asset guarantors are responsible for maintaining a record of the software in accordance with applicable legal regulations and internal regulations of TBU.

(3) The record should contain at least the following information:
a) the name of the software,
b) the supplier or manufacturer of the software
c) the number of licenses purchased,
d) the type of licenses,
e) the validity period of the licenses,
f) the person responsible for the use of the licenses.

(4) The primary asset guarantors are responsible for the distribution, installation, maintenance, modifications, development, and decommissioning of the software.

(5) The deployment of software must comply with the licensing terms and relevant legislation.

II Rules and procedures for monitoring compliance with licensing terms

(6) The process for monitoring compliance with software licensing terms shall be governed and duly documented by the designated primary asset guarantors.

(7) The primary asset guarantors shall conduct regular audits to ensure compliance with licensing terms, including the proposal of appropriate corrective measures.

(8) The primary asset guarantor shall coordinate and collaborate with the supporting asset guarantors in all matters relating to software deployment, registration and the monitoring of compliance with licensing terms.

Document version			
Date	Version	Changed	Description of change
15 May 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.