Code:	SR/14/2025	
Ref. No.:	UTB/24/018650	
Type of document:	INTERNAL	
Category:	RECTOR’S DIRECTIVE	
Title:	Malicious Code Protection Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	7 April 2025	Version: 01
Effective from:	1 May 2025	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services, Data Protection Officer	
Pages:	3	
Appendices:	0	
Distribution list:	TBU employees	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) The Malicious Code Protection Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* defines and deals with the requirements for cyber security 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 establish a procedure to minimise the risks associated with the introduction of malicious code or other unwanted malicious software at TBU.

(3) This policy shall apply to all TBU employees, to information assets used within TBU, and to users of these assets, and the term “users” refers to students, employees with a concluded employment contract or agreement on work performed outside regular employment (hereinafter referred to as “TBU employees”), Emeritus Professors and scholarship holders under concluded cooperation agreements.

(4) Where appropriate, this policy shall also apply to employees of major suppliers and third parties under a concluded contractual relationship for the provision of services or products.

(5) 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
Rules and procedures for the protection of network communications

(1) The protection of network communications shall be systematically ensured and continuously updated by a set of technological means throughout the TBU network.

(2) Network communication protection tool settings and change processes shall be documented and managed.

(3) Communication between network segments shall be controlled by a malicious code protection tool and measures shall be taken to prevent and detect malicious code.

(4) Event logs from the network communication protection tool shall be stored centrally in accordance with the *Asset Management Policy*.

(5) The implementation of the protection of network communications against malicious code is assigned to the Information Technology Centre (hereinafter referred to as "ITC") in accordance with the *Organizational Regulations of the TBU Rectorate,* as amended.

Article 3
Policies and procedures for the protection of servers and shared data storage

(1) A central tool for the protection against malicious code shall be used to protect servers and shared data storage and measures shall be taken to prevent and detect malicious program code.

(2) Server and shared data storage protection tool settings and change processes shall be documented and managed.

(3) Measures shall be put in place to detect, prevent and recover infected data, giving priority to the deletion of the infected file over its treatment.

(4) Event logs (malicious code detection) from server protection tools and shared data storage shall be stored centrally.

(5) The implementation of the protection of servers and shared data storage against malicious code is the responsibility of asset guarantors, IT administrators at the component parts and employees of major suppliers and third parties under a contractual relationship for the provision of services or products.

Article 4
Rules and procedures for workstation protection

(1) A malicious code protection tool shall be included in the software of each workstation and shall be updated regularly and centrally.

(2) Measures shall be put in place to detect, prevent and recover infected data, giving priority to the deletion of the infected file over its treatment.

(3) Event logs (malicious code detection) from the workstation protection tool shall be stored centrally.

(4) Users are prohibited from changing the configuration of the workstation's malicious code protection tool.

(5) The malicious code protection policy is part of the security awareness of users.

(6) Central distribution and updating of the workstation malicious code protection tool is assigned to the Information Technology Centre in accordance with the *Organizational Regulations of the TBU Rectorate*, as amended.

Document version			
Date	Version	Changed	Description of change
7 April 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.