Code:	SR/8/2026	
Ref. No.:	UTB/26/009914	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Physical Security 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:	Physical Security Manager, Technical Services, Information Technology Centre, Legal Services	
Pages:	3	
Appendices:	0	
Distribution list:	TBU employees	
Signature of authorised person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) The Physical Security Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* establishes rules and procedures to ensure the physical security of assets 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 ensure the secure operation of information processing facilities, services and processes in accordance with security requirements and needs. For the purposes of this Policy, ensuring security means preventing damage to, theft or misuse of assets, or disruption to the provision of regulated services to TBU.

(3) This Policy applies to information assets created or used within TBU and to the users of such assets. 'Users' shall mean students, employees engaged under an employment contract or other work agreement (hereinafter referred to as "TBU employees"), emeritus professors, and scholarship holders engaged under cooperation agreements; and, as appropriate, employees of third parties who may, under predefined conditions, enter the protected premises of TBU.

(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
Rules for the protection of buildings and premises

(1) The area in which information is stored and processed and in which technical assets of regulated information systems (IS) are located constitutes a physical security perimeter, which shall be defined, protected and secured:

a. against unauthorised access,
b. against damage and unauthorised interference, and
c. to ensure protection at the level of buildings and within buildings.

(2) For the purposes of physical security, a classification of premises shall be established and documented using the CARVER method, together with the minimum scope of organisational measures and the scope of technical protection systems in areas where information and communication technology components are located:

a. Category "I" premises – premises protected by the highest level of security, requiring enhanced protective measures with precisely defined access rules, monitoring, and the use of certified mechanical barrier systems and intruder alarm and emergency systems (hereinafter referred to as "IAS");
b. Category "II" premises – a building or area protected by a medium level of security. This requires basic protection in order to prevent an attacker from accessing protected assets through clearly defined access rules;
c. Category "III" premises – a building or area protected by an adequate level of security with a lower level of measures directly affecting the movement of persons;
d. Category "IV" premises – a building or area protected only by the necessary safeguards.

(3) The category of specific premises shall be determined by the Physical Security Manager in cooperation with the relevant Asset Guarantors.

(4) Any breach of the physical security in areas where regulated IS information is stored and processed shall be considered a cyber security event or incident and shall be documented and managed in accordance with the rules set out in the *Policy on the Deployment and Use of Tools for the Detection of Cyber Security Incidents*.

Article 3
Rules for controlling access of persons

(1) Buildings in which technical assets of information and communication systems are located shall be secured against access by unauthorised persons by means of established security measures.

(2) Upon detection of an incident (movement of an unauthorised person in an area containing technical assets of information and communication systems), a procedure shall be established and implemented to inform the Physical Security Manager and the facility manager. This procedure is part of regular employee training in accordance with the Security Awareness Development Plan.

(3) Security measures shall be regularly reviewed, updated or, where appropriate, revoked.

Article 4
Rules for the protection of equipment

(1) Technical assets of information and communication systems (e.g. in server rooms and designated data facilities) shall be secured against access by unauthorised persons and shall be located in such premises as to prevent their theft.

(2) Requirements for the protection of equipment to ensure the security of TBU workplaces shall be set out in the individual operating regulations prepared separately for each building. Where server rooms or data facilities are located within a building, specific operating regulations shall be prepared for them separately. All operating regulations shall include, inter alia, permitted access rights and a list of persons who have been assigned privileges for the management of equipment.

Article 5
Detection of breaches of physical security

(1) Breaches of physical security shall be detected by physical security personnel and/or by a detection system connected to the IAS control panel. Where breaches of physical security are detected by employees of TBU, they shall be obliged to inform physical security personnel or, where appropriate, the Police of the Czech Republic. The procedure for reporting security incidents shall be formally described in the operating regulations of the relevant building.

(2) Monitoring of areas containing technical assets of information and communication systems shall fall within the remit of the Technical Services department (hereinafter referred to as the "TS"), which shall immediately notify the designated manager of the relevant premises of any detected breach.

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.