Code:	SR/22/2025	
Ref. No.:	UTB/25/050857	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Policy for the Secure Use of Cryptographic Protection	
Liability:	Tomas Bata University in Zlín	
Issue date:	8 September 2025	Version: 01
Effective from:	15 September 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:	Tomas Bata University in Zlín	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) Policy for the Secure Use of Cryptographic Protection as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* lays down rules and procedures for secure use of cryptographic protection 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) This policy shall apply to all users and information 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.

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

(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
Level of protection with regard to the type and strength of the cryptographic algorithm

(1) The level of protection using a cryptographic algorithm is documented and managed for each piece of software and technical equipment of the supporting asset.

(2) Based on an analysis of the risks of primary assets, the required level of protection is determined, taking into account:

a) the categorization of primary asset information,
b) the use of transmission media,
c) the type and strength of the cryptographic algorithm.

(3) The Information Technology Centre (hereinafter referred to as "ITC") is responsible for documenting and managing the level of protection using a cryptographic algorithm.

Article 3
Rules for cryptographic protection of information

(1) The rules for the use of cryptographic protection are documented and managed by the ITC.

(2) Only currently resistant cryptographic algorithms and cryptographic keys may be used.

(3) Cryptographic algorithms are updated at least in accordance with the valid recommendations of the National Cyber and Information Security Agency (hereinafter referred to as "NÚKIB"). IT administrators at component parts are required to comply with these recommendations when managing supporting assets, which they shall document to the Primary Asset Guarantor in the audit record by the end of the year in which the change occurred.

(4) Cryptographic measures are used for selected assets to ensure:

a) identification and authentication means,
b) authorization means,
c) information transfer,
d) file encryption,
e) security of electronic mail and Internet access.

(5) Cryptographic information protection measures are implemented during transmission over the communication and data network (hereinafter referred to as the "TBU network") and in accordance with the *Communication Network Security Policy*:

a) when accessing the internal TBU network from an external environment,
b) when exchanging information between systems used within the activities of TBU and external entities.

(6) Cryptographic information protection measures are implemented when storing files on mobile devices or removable data carriers only in exceptional cases and in cooperation with the Supporting Asset Guarantors, who keep records of such cases. One of the following methods is used:

a) full disk encryption,
b) virtual disk-level encryption,
c) file-level encryption.

(7) Measures are used to protect electronically transmitted information in accordance with the *Asset Management Policy*, as amended, and the *Secure Information Transfer and Exchange Policy*, as amended. The transfer of information with external entities (e.g., contracting parties) must be carried out in accordance with the *Supplier Management Policy*, as amended.

Article 4
Key management system

(1) As of the date of issuance of this Directive, the key management system has not been implemented at TBU.

Document version			
Date	Version	Changed	Description of change
8 September 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 original document.