Code:	RR/6/2026	
Ref. No.:	UTB/26/033665	
Category:	RECTOR'S DECREE	
Type of document:	INTERNAL	
Title:	Implementation of Multi-Factor Authentication at TBU	
Liability:	Tomas Bata University in Zlín	
Issue date:	14 May 2026	Version: 01
Effective from:	15 May 2026	
Issued by:	Rector	
Prepared by:	Bursar	
In cooperation with:	TBU Legal Services, Information Technology Centre	
Pages:	3	
Appendices:	0	
Distribution list:	TBU employees, TBU students	
Signature of authorised person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) This Rector's Decree regulates the implementation of multi-factor authentication (hereinafter referred to as "MFA") at Tomas Bata University in Zlín (hereinafter referred to as "**TBU**") for the purpose of increasing the level of cyber security of information systems, data, and user accounts.

(2) The implementation of MFA is based primarily on:
a) the requirements of the relevant legal regulations concerning cyber security,
b) recommendations of the National Cyber and Information Security Agency (hereinafter referred to as "NÚKIB"),
c) recommendations of the TBU Cyber Security Management Committee,
d) the assessment of security risks related to unauthorised access, phishing attacks, and the compromise of user accounts.

Article 2
Obligation to use MFA

(1) Employees and students of TBU (hereinafter referred to as "**users**") are required to use multi-factor authentication when logging into selected TBU information systems.

(2) MFA shall be required:
a) for remote access via VPN,
b) when changing passwords,
c) for selected cloud services and single sign-on systems.

(3) At TBU, the use of MFA may subsequently be gradually extended to additional systems based on ongoing security risk assessments, with the aim of minimising disruption to operational continuity.

Article 3
How MFA works

(1) MFA represents a security process in which, in addition to a username and password, further verification of the user's identity is required.

(2) MFA is based on a combination of at least two independent factors:
a) something the user knows (password or PIN),
b) something the user possesses (mobile phone, authentication application, token),
c) something the user is (biometric data).

(3) The second authentication factor may include in particular:
a) a one-time password (OTP) code generated by an authentication application,
b) an SMS message containing a verification code,
c) a hardware security token,
d) biometric verification.

Article 4
Authentication applications

(1) For MFA at TBU, the use of authentication applications such as the following is recommended:
a) Microsoft Authenticator,
b) Google Authenticator,
c) other similar applications.

(2) These applications allow the generation of OTP codes even without an internet connection.

(3) MFA registration is carried out by scanning a QR code during the user account activation process.

(4) Detailed instructions for MFA activation, a list of supported authentication applications, technical requirements, and technical support contacts are published on the website of the Information Technology Centre (hereinafter referred to as "**ITC**").

(5) TBU prefers the use of authentication applications on users' mobile devices; however, in the cases specified below, it shall provide an alternative method of multi-factor authentication.

(6) For users who cannot or do not wish to use a smart mobile device, the ITC shall provide an alternative method of multi-factor authentication, in particular through:
a) a desktop authentication application,
b) a hardware security token,
c) another technically supported authentication method.

The specific alternative authentication method shall be determined with regard to technical capabilities, security requirements, and the nature of the user's job position.

Article 5
User obligations

(1) Users are required to:
a) protect their authentication credentials,

b) not provide OTP codes or other authentication credentials to third parties,
c) immediately report any suspected account misuse or loss of a device or authentication credential to the ITC,
d) follow the ITC's instructions when activating and using MFA.

Article 6
Obligations of the ITC

(1) The ITC shall:
a) ensure the technical implementation of MFA,
b) provide methodological support to users,
c) publish MFA activation procedure,
d) provide support for MFA registration and use.

Article 7
Final provisions

The ITC is responsible for monitoring compliance with this Decree.

Document version			
Date	Version	Changed	Description of change
14 May 2026	01	Bursar	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.