

Kód:	RR/6/2026	
Číslo jednací:	UTB/26/033665	
Druh:	ROZHODNUTÍ REKTORA	
Klasifikace dokumentu:	INTERNÍ	
Název:	Zavedení multifaktorové autentizace na UTB	
Organizační závaznost:	Univerzita Tomáše Bati ve Zlíně	
Datum vydání:	14. 5. 2026	Verze: 01
Účinnost:	15. 5. 2026	
Vydává:	Rektor	
Zpracoval:	Kvestorka	
Spolupracoval:	Právní oddělení, CVT	
Počet stran:	3	
Počet příloh:	0	
Rozdělovník:	Zaměstnanci UTB, studenti UTB	
Podpis oprávněné osoby:	prof. Mgr. Milan Adámek, Ph.D., v. r.	

Článek 1 Úvodní ustanovení

- (1) Toto rozhodnutí rektora upravuje zavedení multifaktorové autentizace (dále jen „**MFA**“) na Univerzitě Tomáše Bati ve Zlíně (dále jen „**UTB**“) za účelem zvýšení úrovně kybernetické bezpečnosti informačních systémů, dat a uživatelských účtů.
- (2) Zavedení MFA vychází zejména:
- a) z požadavků příslušných právních předpisů týkajících se kybernetické bezpečnosti,
 - b) z doporučení Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“),
 - c) z doporučení Výboru pro řízení kybernetické bezpečnosti UTB,
 - d) z vyhodnocení bezpečnostních rizik v oblasti neoprávněných přístupů, phishingových útoků a kompromitace uživatelských účtů.

Článek 2 Povinnost využívání MFA

- (1) Zaměstnanci a studenti UTB (dále jen „**uživatelé**“) jsou povinni využívat multifaktorovou autentizaci při přihlašování do vybraných informačních systémů UTB.
- (2) MFA bude vyžadována:
- a) pro vzdálený přístup prostřednictvím VPN,
 - b) při změně hesla,
 - c) pro vybrané cloudové služby a systémy jednotného přihlášení.
- (3) Na UTB může následně docházet k postupnému rozšiřování využití MFA na další systémy v návaznosti na vyhodnocování bezpečnostních rizik s cílem minimálního narušení kontinuity provozu.

Článek 3

Princip fungování MFA

- (1) MFA představuje bezpečnostní proces, při kterém je kromě uživatelského jména a hesla vyžadováno také další ověření identity uživatele.
- (2) MFA je založena na kombinaci alespoň dvou nezávislých faktorů:
 - a) něco, co uživatel zná (heslo nebo PIN),
 - b) něco, co uživatel vlastní (mobilní telefon, autentizační aplikace, token),
 - c) něco, čím uživatel je (biometrický údaj).
- (3) Druhým ověřovacím prvkem může být zejména:
 - a) jednorázový OTP (**One -Time Password**) kód generovaný autentizační aplikací,
 - b) SMS zpráva s ověřovacím kódem,
 - c) hardwarový bezpečnostní token,
 - d) biometrické ověření.

Článek 4

Autentizační aplikace

- (1) Pro MFA na UTB se doporučuje využití autentizačních aplikací typu:
 - a) Microsoft Authenticator,
 - b) Google Authenticator,
 - c) jiné obdobné aplikace.
- (2) Aplikace umožňují generování jednorázových OTP kódů i bez připojení k internetu.
- (3) Registrace MFA probíhá prostřednictvím načtení QR kódu v procesu aktivace uživatelského účtu.
- (4) Podrobný postup aktivace MFA, seznam podporovaných autentizačních aplikací, technické požadavky a kontakty na technickou podporu jsou zveřejněny na webových stránkách Centra výpočetní techniky (dále jen „CVT“).
- (5) UTB preferuje využití autentizačních aplikací na mobilních zařízeních uživatelů, avšak v níže uvedených případech zajistí alternativní způsob vícefaktorového ověření.
- (6) Uživatelům, kteří nemohou nebo nechtějí využívat chytré mobilní zařízení, umožní CVT alternativní způsob vícefaktorového ověření, zejména prostřednictvím:
 - a) desktopové autentizační aplikace ,
 - b) hardwarového bezpečnostního tokenu,
 - c) jiného technicky podporovaného způsobu ověření.

Konkrétní alternativní způsob autentizace je stanoven s ohledem na technické možnosti, bezpečnostní požadavky a charakter pracovního zařazení uživatele.

Článek 5

Povinnosti uživatelů

Uživatelé jsou povinni:

- a) chránit své autentizační prostředky,
- b) neposkytovat OTP kódy ani jiné autentizační údaje třetím osobám,
- c) bezodkladně oznámit CVT podezření na zneužití účtu nebo ztrátu zařízení nebo autentizačního prostředku,
- d) postupovat dle pokynů CVT při aktivaci a používání MFA.

Článek 6

Povinnosti CVT

CVT:

- a) zajistí technickou implementaci MFA,
- b) poskytne uživatelům metodickou podporu,
- c) zveřejní postup aktivace MFA,
- d) zajistí podporu při registraci a používání MFA.

Článek 7

Závěrečná ustanovení

Kontrolou dodržování tohoto rozhodnutí je pověřeno CVT.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny
14. 5. 2026	01	kvestorka	Vytvoření dokumentu