

Kód:	SR/13/2026	
Číslo jednací:	UTB/26/012127	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika bezpečného chování uživatelů	
Organizační závaznost:	Univerzita Tomáše Bati ve Zlíně	
Datum vydání:	16.02.2026	Verze: 01
Účinnost:	20.02.2026	
Vydává:	Rektor	
Zpracoval:	Manažer kybernetické bezpečnosti	
Spolupracoval:	Centrum výpočetní techniky, Právní oddělení, Kvestor	
Počet stran:	5	
Počet příloh:	0	
Rozdělovník:	zaměstnanci UTB	
Podpis oprávněné osoby:	prof. Mgr. Milan Adámek, Ph.D., v.r.	

Článek 1 Úvodní ustanovení

- (1) Politika bezpečného chování uživatelů jako součást *Deklarace kybernetické bezpečnosti Univerzity Tomáše Bati ve Zlíně* stanovuje pravidla chování uživatelů za účelem zajištění bezpečnosti informací a snížení rizik výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události a rozpracovává požadavky na kybernetickou bezpečnost dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“) a souvisejících právních předpisů v podmínkách Univerzity Tomáše Bati ve Zlíně (dále jen „UTB“).
- (2) Účelem této politiky je definovat zásady bezpečného chování uživatelů, stanovit povinnosti uživatelů a definovat pravidla bezpečného provozu významných informačních systémů (dále jen „VIS“). Uživatelé se rozumí studenti, zaměstnanci s uzavřenou pracovní smlouvou nebo dohodou (dále jen „zaměstnanci UTB“), emeritní profesori a stipendisté na základě uzavřených dohod o spolupráci a přiměřeně také zaměstnanci významných dodavatelů a třetích stran na základě uzavřeného smluvního vztahu na dodávku služeb nebo produktů.
- (3) Jednotlivé pojmy používané v této politice jsou vymezeny zejména zákonem o kybernetické bezpečnosti a vyhláškou o kybernetické bezpečnosti. Přehled jednotlivých pojmů je uveden v dokumentu *Základní pojmy kybernetické bezpečnosti*, který je dostupný na webu UTB v sekci *Kybernetická bezpečnost*.

Článek 2

Pravidla pro bezpečné nakládání s aktivy VIS

- (1) Pravidla pro zacházení s aktivy VIS jsou stanovena jejich klasifikací a jsou dokumentována pro každé aktivum v souladu s klasifikací aktiv uvedenou v *Příloze č. 1* směrnice rektora *Politika řízení aktiv* v platném znění.
- (2) Uchovávání, ukládání a archivace informací, dat a procesů specifikovaných v odstavci 1 jsou uživatelé povinni provádět tak, aby byla zajištěna jejich dostatečná ochrana před neoprávněným přístupem a aby bylo znemožněno jejich zneužití.
- (3) Každý uživatel je povinen:
 - a) uzamknout své koncové zařízení s otevřeným přístupem/aktivním přihlášením (k aktivům VIS) při každém opuštění pracoviště,
 - b) ukončit aktivní přístup (odhlášení) ke všem aktivům VIS při skončení své pracovní směny.
- (4) Každý uživatel má přístup pouze k těm aktivům VIS, která nezbytně potřebuje k výkonu svých činností.
- (5) Případné výjimky z pravidel jsou realizovány na základě odůvodněné a schválené žádosti. Žádost schválí přímý nadřízený a vedoucí zaměstnanec součásti žadatele a postoupí ji Manažerovi kybernetické bezpečnosti (dále jen „Manažer KB“), který ji schválí nebo zamítne. Pokud Manažer KB žádost schválí, postoupí ji řediteli Centra výpočetní techniky UTB (dále jen „CVT“) k technické realizaci.

Článek 3

Bezpečné použití přístupového hesla

- (1) Heslem se pro účely této politiky rozumí kombinace znaků a/nebo číslic, tedy včetně kódu (PIN).
- (2) Uživatelé musí uchovávat a používat hesla takovým způsobem, aby nebyla vyražena jiným osobám.
- (3) Hesla používaná pro přístupy k informačním systémům UTB nesmí uživatel používat pro služby, aplikace a systémy využívané k soukromým účelům.
- (4) Uživatelé jsou o aktuálních parametrech jednotlivých pravidel tvorby silného hesla informováni při registraci, případně při změně hesla.
- (5) Pravidla tvorby hesel stanovují minimálně tyto parametry:
 - a) minimální délka hesla,

- b) použití kombinace malých, velkých písmen, číslic a speciálních znaků,
 - c) možnost vyžádané změny hesla,
 - d) povinná změna hesla po určité době,
 - e) zákaz tvorby hesla ze skutečnosti, kterou může někdo snadno odhadnout nebo ji získat z osobních informací, např. jméno, příjmení, datum narození, rodné číslo apod., nenapadnutelnost slovníkovým útokem (tj. neskládají se ze slov obsažených ve slovníku), zákaz shody s přihlašovacím jménem,
 - f) nemožnost použít opakovaně stejné heslo při jeho změně.
- (6) Pravidla pro vytváření a používání hesel mohou být vymáhána přímo systémovými prostředky.

Článek 4

Bezpečné použití elektronické pošty a přístupu na internet

- (1) V rámci elektronické pošty jsou nastavena následující pravidla:
- a) informace obsažené v elektronicky předávaných zprávách je nutno chránit podle *Klasifikace aktiv UTB*,
 - b) uživatelé mohou používat elektronickou poštu pouze ke studijním a/nebo pracovním účelům,
 - c) u informací s vysokou úrovní důvěrnosti jsou vyžadovány kryptografické prostředky pro jejich ochranu.
- (2) Při použití elektronické pošty je zakázáno:
- a) používat prostředky elektronické pošty UTB pro soukromé účely,
 - b) zaměstnancům UTB používat k pracovním účelům veřejné e-mailové služby (např. Gmail, Seznam apod.),
 - c) zasílat nechráněné osobní nebo citlivé údaje prostým e-mailem včetně nešifrovaných příloh obsahujících osobní údaje či citlivá data,
 - d) otevírat přílohy a webové odkazy z e-mailů od neznámých či nedůvěryhodných zdrojů; v případě výskytu podezřelého e-mailu je uživatel povinen nahlásit tuto skutečnost na adresu helpdesku abuse@utb.cz,
 - e) nastavovat pravidla pro automatické přeposílání elektronické pošty mimo UTB.
- (3) Před ukončením pracovního poměru nebo dohody je zaměstnanec UTB povinen v případě své osobní e-mailové schránky (uzivatel@utb.cz):
- a) Zajistit předání pracovní agendy,
 - b) zajistit nastavení automatické odpovědi s uvedením kontaktů na přímého vedoucího zaměstnance,
 - c) odstranit nebo předat data v souladu s vnitřními normami UTB.

- (4) Po ukončení pracovního poměru nebo dohody může být zaměstnanci ponechán přístup k pracovní e-mailové schránce po dobu nejvýše 60 kalendářních dnů, a to výhradně za účelem předání agendy a zajištění kontinuity činností UTB, nerozhodne-li přímý vedoucí zaměstnanec, že přístup ponechán nebude. Jakékoliv jiné využití pracovní e-mailové schránky je zakázáno.
- (5) Pokud měl zaměstnanec s ukončeným pracovním poměrem nebo dohodou přístup k obecné univerzitní e-mailové schránce, odpovídá přímý vedoucí zaměstnanec za její správné nastavení včetně změny přístupových údajů.
- (6) V rámci přístupu na internet je zakázáno:
 - a) používat služeb internetu pro jiné než studijní a pracovní účely,
 - b) ukládat aktiva VIS na neschválená veřejná úložiště podle směrnice rektora *Ochrana a zpracování osobních údajů* v platném znění,
 - c) stahovat z nedůvěryhodných a neověřených zdrojů spustitelné soubory a soubory obsahující makra.

Článek 5

Bezpečný vzdálený přístup

- (1) Bezpečný vzdálený přístup do vnitřních sítí je dokumentovaný a řídí se těmito pravidly
 - a) pro vzdálený přístup k aktivům VIS musí uživatelé využít výhradně Virtual Private Network (dále jen „VPN“) provozovanou UTB,
 - b) pro využívání aktiv VIS prostřednictvím vzdáleného přístupu platí stejná pravidla uvedená v politikách kybernetické bezpečnosti, jako pro práci na pracovišti,
 - c) vytvořené spojení v rámci vzdáleného přístupu je šifrované a předchází mu autentizace uživatele,
 - d) přístupy jsou jednoznačně zaznamenány spolu s identifikací uživatele,
 - e) uživatelé nesmí sdílet své oprávnění vzdáleného přístupu.
- (2) Uživatelé prostředků umožňujících vzdálený přístup jsou povinni neprodleně provádět všechny doporučené aktualizace a úpravy prostředků umožňujících vzdálený přístup tak, aby byla minimalizována rizika jejich zneužití pro neoprávněný přístup k aktivům VIS.

Článek 6

Bezpečné chování na sociálních sítích

- (1) Uživatelé, kteří nemají v popisu práce využívání a správu oficiálních účtů UTB na sociálních sítích, nejsou oprávněni přístup k sociálním sítím využívat.
- (2) Uživatelé, do jejichž pracovní náplně spadá využívání a správa oficiálních účtů UTB na sociálních sítích, dodržují pravidla bezpečné práce se sociálními sítěmi, zejména:

- a) chrání přihlašovací údaje, dodržují dostatečnou komplexnost hesla, jeho důvěrnost a pravidelnou obměnu,
- b) využívají sociální sítě pouze pro oficiální potřeby UTB a sdílejí pouze takové informace, které jsou v souladu s oficiální komunikační politikou, ochranou osobních údajů a zájmy UTB,
- c) používají virtuálně oddělené prostředí či uživatelský profil.

Článek 7

Bezpečnost ve vztahu k mobilním zařízením

- (1) Bezpečnost ve vztahu k mobilním zařízením se řídí směrnicí rektora *Politika bezpečného používání mobilních zařízení* v platném znění.

Článek 8

Závěrečná ustanovení

- (1) Tato směrnice nahrazuje směrnicí rektora č. 5/2025.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny
16.02.2026	01	Manažer KB	Vytvoření dokumentu