

Kód:	SR/11/2026	
Číslo jednací:	UTB/26/012123	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika bezpečnosti komunikační sítě	
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:	7	
Počet příloh:	0	
Rozdělovník:	Univerzita Tomáše Bati ve Zlíně	
Podpis oprávněné osoby:	prof. Mgr. Milan Adámek, Ph.D., v.r.	

Článek 1 Úvodní ustanovení

- (1) Politika bezpečnosti komunikační sítě jako součást *Deklarace kybernetické bezpečnosti Univerzity Tomáše Bati ve Zlíně* stanovuje způsoby ochrany komunikační a datové sítě (dále jen „sít' UTB“) 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 stanovit způsob ochrany sítě UTB pro zajištění správného a bezpečného provozu.
- (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 Sít' UTB

- (1) UTB provozuje a spravuje neveřejnou sít' určenou k přenosu digitálních dat pro zajištění vlastních elektronických služeb a pro zajištění přístupu k interním i externím digitalizovaným zdrojům.
- (2) Sítí UTB se rozumí všechny technické a programové prostředky, které slouží k propojení zařízení a k využití tohoto propojení. Sít' UTB je distribuovaná do jednotlivých lokalit, areálů a objektů UTB a je členěná na jednotlivé subsítě.

- (3) Síť UTB je připojena do sítě Internet prostřednictvím národní e-infrastruktury pro vědu a výzkum, kterou provozuje sdružení CESNET z. s. p. o., jehož je UTB členem.
- (4) Uživateli sítě UTB (dále jen „uživatel“) se rozumí:
- a) studenti UTB (dále jen „studenti“) a zaměstnanci s uzavřenou pracovní smlouvou nebo dohodou o pracích konaných mimo pracovní poměr (dále jen „zaměstnanci UTB“), kteří mají zřízen uživatelský účet pro přístup do sítě UTB, a přímo užívají výše zmíněné síť UTB či zařízení k nim připojená,
 - b) emeritní profesori, stipendisté, hosté a další uživatelé využívajících síť UTB na základě příslušných roamingových nebo jiných smluv,
 - c) přiměřeně také zaměstnanci významných dodavatelů a třetích stran na základě uzavřeného smluvního vztahu na dodávku služeb nebo produktů.
- (5) Termínem uživatelský účet (dále jen „účet“) se rozumí oprávnění pracovat na daném zařízení nebo v síti UTB s jednoznačnou identifikací uživatele. Obvykle se jedná o uživatelské jméno a heslo.

Článek 3

Přístup k síti UTB a identifikace uživatele

- (1) Každý uživatel podle článku 2, odstavce 4 bodu a) má zřízen účet pro přístup do sítě UTB. Účet se zřizuje na základě zavedení uživatele do odpovídající evidence (SAP, IS/STAG). V odůvodněných případech mohou mít uživatelé v síti UTB více účtů.
- (2) Novému uživateli je automaticky přiděleno uživatelské jméno a přístupové heslo. Každý uživatel je povinen si toto přidělené přístupové heslo změnit.
- (3) Ukončením pracovního poměru, dohody, ukončením nebo přerušením studia zaniká uživateli právo na používání sítě UTB. Tím není dotčena možnost časově omezeného přístupu k pracovní e-mailové schránce v souladu se směrnicí rektora týkající se politiky bezpečného předávání a výměny informací.

Článek 4

Určení práv a povinností uživatelů sítě UTB

- (1) Uživatelé sítě UTB smí využívat prostředky sítě UTB ve shodě se svými pracovními a studijními povinnostmi, a to především pro vzdělávací, vědecké, výzkumné, vývojové, inovační, umělecké a další tvůrčí činnosti nebo povinnosti související se zajištěním provozu a správy UTB. Přitom musí důsledně respektovat vlastnická práva k datům uloženým v elektronické podobě.
- (2) Zaměstnanci významných dodavatelů a třetích stran smí využívat prostředky sítě UTB výhradně pro plnění povinností vyplývajících z uzavřených smluv na dodávku služeb nebo produktů.

- (3) Je zakázáno používat síť UTB pro komerční účely, šíření obchodních informací, politickou, náboženskou nebo rasovou agitaci, propagaci drog a šíření materiálů, které jsou v rozporu se zákonem.
- (4) Při komunikaci s jinými sítěmi je uživatel povinen dodržovat pravidla, která platí v těchto sítích a dodržovat *Podmínky přístupu k e-infrastruktuře CESNET* v platném znění (www.cesnet.cz).
- (5) Všechny prostředky sítě UTB jsou vlastnictvím UTB, případně k nim UTB vlastní či vykonává práva užívání. Nepřípustnost krádeže a vandalismu (poškození) se vztahuje na elektronickou podobu dat a informací, stejně jako na vlastní fyzické prostředky.
- (6) Uživatelé sítě UTB jsou povinni zejména:
 - a) chránit svůj uživatelský účet heslem v souladu s *Politikou bezpečného chování uživatelů*,
 - b) technické prostředky, které pro své připojení k síti UTB využívají, chránit před zneužitím a na nich používaný software (zejména operační systém a ochranné programy) udržovat v aktuálním stavu,
 - c) počínat si tak, aby nezpůsobili vniknutí škodlivého software do sítě UTB a jeho šíření,
 - d) informovat správce sítě UTB o odhalených nedostatcích v bezpečnosti sítě UTB, a případných závadách hardware,
 - e) nevytvářet nadměrné datové toky vedoucí k zatížení sítě UTB.
- (7) Uživatelům sítě UTB je zakázáno zejména:
 - a) připojovat do sítě UTB jakékoliv aktivní prvky (zejména směrovače, přepínače, přístupové body apod.) nebo servery bez předchozí konzultace se správcem sítě UTB a jeho písemného souhlasu,
 - b) připojovat do sítě UTB zařízení, která nesplňují požadavky platných norem a která mohou způsobit ohrožení zdraví nebo života osob, poškození sítě UTB nebo jiného majetku nebo negativně ovlivnit provoz sítě UTB,
 - c) zasahovat jakýmkoli způsobem do kabeláže a propojujících prvků sítě UTB, včetně jejich vypínání bez závažných důvodů.
 - d) poškozovat nebo umožnit poškození nebo zničení softwarového či hardwarového vybavení sítě UTB.
 - e) instalovat bez schválení správce sítě UTB softwarové vybavení neúměrně zvyšující zatížení sítě UTB a serverů,
 - f) neoprávněně instalovat, rozmnožovat nebo sdělovat veřejnosti prostřednictvím sítě UTB díla, počítačové programy, databáze a další výsledky duševní tvůrčí činnosti, které jsou chráněny právem duševního vlastnictví (zejména autorským zákonem, zákonem o zpracování osobních údajů a zákonem o utajovaných informacích a bezpečnostní způsobilosti),
 - g) neautorizované kopírování i částí softwarového vybavení nebo dat, k nimž UTB vykonává vlastnická práva, resp. práva k užívání,
 - h) neautorizovaná modifikace softwaru, dat nebo technického vybavení v majetku či užívání UTB, zvláště přísně jsou pak zakázány neautorizované změny konfigurace počítačů či jiných prostředků, které by mohly mít vliv na provoz nebo bezpečnost celé sítě UTB,

- i) vědomě používat a šířit jakoukoliv cestou soubory se škodlivým softwarem a tím narušovat bezpečnost dat v síti UTB,
- j) pokoušet se o průnik do systémů, k jejichž využívání uživatel není oprávněn,
- k) zprostředkovávat přístup k síti UTB a k dalším službám sítě UTB neoprávněným fyzickým nebo právníckým osobám,
- l) poskytnout přidělené uživatelské jméno a své heslo k účtu jiné osobě; za hrubé porušení pravidel se považuje jejich poskytnutí osobě, která nemá nárok na přístup do sítě UTB nebo které byl tento přístup z jakýchkoliv důvodů zablokován,
- m) pracovat pod cizí identitou, včetně rozesílání elektronické pošty pod cizí identitou, nebo zneužívat nedbalosti jiných uživatelů (např. opomenutí odhlášení, nevhodná ochrana souborů) k přístupu k cizím datům nebo informacím a používat takové softwarové prostředky, které mohou vést k získání cizí identity,
- n) pokoušet se získat přístupová práva, která mu nebyla přidělena; pokud uživatel získá taková práva chybou softwaru či hardwaru, je povinen na tuto skutečnost neprodleně upozornit svého přímého nadřízeného zaměstnance,
- o) odposlouchávat provoz a vytvářet kopie zpráv procházejících jednotlivými síťovými zařízeními, pokud nejde o výkon takové činnosti v rámci výuky specializovaných předmětů odborným ústavem/ateliérem, přičemž tato činnost musí být prováděna výhradně v prostorách tohoto ústavu/ateliéru k tomu určeným a za podmínek, které určí jednotlivý vyučující, případně garanti vyučovaných předmětů,
- p) využívat prostředků sítě UTB k činnostem uvedeným v bodech a) až o) namířeným proti jakékoliv další organizaci, jejíž komunikační prostředky jsou dostupné prostřednictvím sítě UTB,
- q) využívat síť UTB v rozporu s platnými zákony a k páčání přestupků a trestných činů.

Článek 5

Určení práv a povinností za bezpečný provoz sítě UTB

- (1) Správa sítě UTB přísluší podle *Organizačního řádu Rektorátu UTB* v platném znění Centru výpočetní techniky (dále jen „CVT“).
- (2) Správcem sítě UTB (dále jen „správce sítě“) je osoba nebo osoby pověřené správou prostředků sítě UTB a zodpovědné za jejich provoz.
- (3) CVT odpovídá za provoz páteřní sítě UTB, funkčnost připojení jednotlivých součástí UTB, provoz centrálních síťových služeb a serverů, spravuje adresní prostor a přiděluje adresy jednotlivým subsítím.
- (4) CVT metodicky řídí a koordinuje správce IT součástí v oblasti pravidel používání sítě UTB a spolupracuje s nimi při zajišťování služeb sítě UTB v rámci potřeb součástí.
- (5) CVT vede evidenci uživatelů, zabezpečuje správu jejich uživatelských účtů, e-mailových adres a přidělování sdíleného síťového diskového prostoru na centrálních serverech.
- (6) CVT má právo:
 - a) odpojit část sítě UTB (subsít'), ke které byly připojeny neschválené technické prostředky nebo na níž byla provedena neschválená změna konfigurace síťového programového

vybavení a tyto prostředky či tato změna vedly k závažným poruchám, které ohrožují provoz nebo bezpečnost sítě UTB;

- b) dočasně omezit přístup ke službám sítě UTB při důvodném podezření z porušování této směrnice;
- c) v případě důvodného podezření ze zneužití uživatelského účtu okamžitě zablokovat uživatelský účet. Informaci o zablokování uživatelského účtu předá CVT neprodleně přímému nadřízenému zaměstnanci nebo studijnímu oddělení příslušné fakulty a příslušnému proděkanovi, v případě uživatelů podle článku 2, odstavce 4, písmene b), c), vedoucímu zaměstnanci příslušné součásti;
- d) stanovit další závazná pravidla upravující specifické činnosti v jednotlivých subsítích sítě UTB.

Článek 6

Pravidla a postupy pro zajištění bezpečnosti sítě UTB

- (1) Každá část sítě UTB musí být dokumentovaná ve fyzické a logické vrstvě za účelem zajištění její bezpečnosti a odolnosti vůči případným kybernetickým útokům.
- (2) Správa sítě UTB a síťových prvků musí být oddělena od správy pracovních stanic a serverů.
- (3) Síť UTB je segmentována a logicky oddělena za účelem zajištění bezpečnosti a odolnosti vůči případným kybernetickým útokům.

Článek 7

Pravidla a postupy pro řízení přístupů v rámci sítě

- (1) Pravidla pro řízení přístupu se aplikují na všechny segmenty Local Area Network (LAN) ve správě UTB.
- (2) Pro přístupy uživatelů a administrátorů do sítě UTB jsou použity nástroje pro správu a ověření identity, pro přístupy technických prostředků do sítě UTB jsou použity nástroje pro správu přístupu k technickým prostředkům.
- (3) Přístupy jsou řízeny na základě skupin a rolí.

Článek 8

Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů

- (1) CVT monitoruje provoz sítě UTB a v odůvodněných případech může monitorovat i činnost konkrétního uživatele.
- (2) Záznamy událostí je nutné uchovávat po dobu vyžadovanou zvláštním právním předpisem (vyhláška o kybernetické bezpečnosti), nejméně však po dobu 12 měsíců.
- (3) Záznamy událostí musí být zajištěny před neoprávněným přístupem a neoprávněnou modifikací.

- (4) Všechny prvky sítě UTB jsou napojeny na určený zdroj přesného času a jsou nejméně jednou za den synchronizovány.
- (5) Vyhodnocování provozních záznamů je plně v kompetenci CVT.

Článek 9

Pravidla a postupy pro ochranu vzdáleného přístupu k síti UTB

- (1) Vzdálený přístup uživatelů k síti UTB je umožněn komunikačním kanálem chráněným kryptografickými prostředky.
- (2) Přístup z externích sítí je možný jen do demilitarizovaných zón (DMZ) navržených tak, aby případný vnější útok neohrozil bezpečnost interní sítě.
- (3) Vzdálené připojení dodavatelů je možné jen na základě uzavřených smluvních vztahů, jejichž obsahem je povinně vzájemně akceptovaná bezpečnostní politika pro taková připojení.
- (4) Bezpečný vzdálený přístup do vnitřních sítí je dokumentovaný a řídí se těmito pravidly:
 - a) pro vzdálený přístup musí uživatelé využít výhradně Virtual Private Network (dále jen „VPN“) provozovanou UTB,
 - b) pro využívání 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.
- (5) 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.

Článek 10

Sankce za nedodržování pravidel provozu sítě UTB

- (1) Správce sítě UTB a administrátor mají právo dočasně omezit, zamezit či zrušit přístup k síti UTB uživatelům, kteří prokazatelně porušili ustanovení této směrnice, a to v rozsahu delegovaných kompetencí a práv.
- (2) Zjištěné méně závažné porušení této směrnice dává správci sítě nebo jím pověřené osobě právo uživatele upozornit na porušování pravidel.
- (3) Zaviněné porušení ustanovení této směrnice bude u studentů považováno za disciplinární přestupek dle § 64 zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, v platném znění. Za disciplinární přestupek lze uložit studentovi sankci

dle ustanovení § 65 citovaného zákona a příslušných ustanovení Disciplinárního řádu pro studenty Univerzity Tomáše Bati ve Zlíně, přičemž za závažný a úmyslně spáchaný disciplinární přestupek může být student až vyloučen ze studia.

- (4) Porušení ustanovení této směrnice bude u zaměstnanců považováno za porušení základních povinností zaměstnance (§ 301, písmeno c) a d) zákona č. 262/2006 Sb. v platném znění – Zákoníku práce) a lze z něj vyvodit příslušné pracovně-právní důsledky až po rozvázání pracovního poměru.
- (5) Případná trestně právní odpovědnost není tímto postupem omezena ani vyloučena.

Článek 11

Závěrečná ustanovení

- (1) Tato směrnice ruší a nahrazuje směrnici rektora č. 13/2025.

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