

Kód:	SR/8/2026	
Číslo jednací:	UTB/26/009914	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika fyzické bezpečnosti	
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:	Manažer fyzické bezpečnosti, Technicko-provozní odbor, Centrum výpočetní techniky, Právní oddělení	
Počet stran:	3	
Počet příloh:	0	
Rozdělovník:	zaměstnanci UTB	
Podpis oprávněné osoby:	prof. Mgr. Milan Adámek, Ph.D., v.r.	

Článek 1 Úvodní ustanovení

- (1) Politika fyzické bezpečnosti jako součást *Deklarace kybernetické bezpečnosti Univerzity Tomáše Bati ve Zlíně* stanovuje pravidla a postupy pro zajištění fyzické bezpečnosti aktiv 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 politiky je zajistit bezpečný provoz prostředků pro zpracování informací, služeb a procesů v souladu s bezpečnostními požadavky a potřebami. Zajištěním bezpečnosti se zde rozumí předcházení poškození, krádeží nebo zneužití aktiv nebo přerušení poskytování regulovaných služeb UTB.
- (3) Tato politika se vztahuje na informační aktiva vytvořená nebo používaná v rámci UTB, a na uživatele těchto aktiv. Uživateli 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 také přiměřeně pro zaměstnance třetích stran, kteří mohou za předem definovaných podmínek do chráněných prostor UTB vstupovat.
- (4) Jednotlivé pojmy používané v této směrnici jsou vymezeny zejména zákonem o kybernetické bezpečnosti a souvisejícími právními předpisy. Přehled jednotlivých pojmů je uveden v dokumentu *Pojmy kybernetické bezpečnosti*, který je dostupný na webu UTB v sekci *Kybernetická bezpečnost*.

Článek 2

Pravidla pro ochranu objektů

- (1) Oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva regulovaných IS jsou fyzickým bezpečnostním perimetrem, který je vymezen, chráněn a zabezpečen:
 - a. před neoprávněným vstupem,
 - b. před poškozením, neoprávněnými zásahy a
 - c. pro zajištění ochrany na úrovni objektů a v rámci objektů.
- (2) Z hlediska fyzické bezpečnosti je stanovena a dokumentována kategorizace prostor metodou CARVER, minimální rozsah organizačních opatření a rozsah systémů technické ochrany, ve kterých jsou umístěny prvky informačních a komunikačních technologií:
 - a. prostory kategorie „I“ – prostor chráněný nejvyšší úrovní zabezpečení, který vyžaduje zvýšenou ochranu zabezpečení s přesně definovaným pravidlem přístupu, jeho monitorováním a s použitím certifikovaných mechanických zábranných systémů a poplachových zabezpečovacích a tísňových systémů (dále jen „PZTS“),
 - b. prostory kategorie „II“ – objekt nebo prostor chráněný střední úrovní zabezpečení. Vyžaduje základní ochranu tak, aby se zabránilo útočníkovi v přístupu k chráněnému aktivu pomocí přesně definovaných pravidel přístupu,
 - c. prostory kategorie „III“ – objekt nebo prostor chráněný přiměřenou úrovní zabezpečení s nižší úrovní opatření majícími přímý vliv na pohyb osob,
 - d. prostory kategorie „IV“ – objekt nebo prostor chráněný pouze nezbytnou ochranou.
- (3) Kategorie konkrétních prostor určuje Manažer fyzické bezpečnosti ve spolupráci s Garanty příslušných aktiv.
- (4) Narušení fyzické bezpečnosti oblastí, kde jsou uchovávány a zpracovávány informace regulovaných IS, se považuje za kybernetickou bezpečnostní událost, případně za kybernetický bezpečnostní incident a je dokumentováno a řízeno v souladu s pravidly stanovenými *Politikou nasazení a používání nástrojů pro detekci kybernetických bezpečnostních událostí*.

Článek 3

Pravidla pro kontrolu vstupu osob

- (1) Objekty, ve kterých se nachází technická aktiva informačních a komunikačních systémů, jsou zabezpečeny proti přístupu neoprávněných osob nastavenými režimovými opatřeními.
- (2) Při zjištění incidentu (pohybu neoprávněné osoby v prostoru s technickými aktivy informačních a komunikačních systémů) je stanoven a prováděn postup, kterým je informování Manažera fyzické bezpečnosti a správce objektu. Tento postup je součástí pravidelného školení zaměstnanců v souladu s Plánem rozvoje bezpečnostního povědomí.
- (3) Režimová opatření jsou pravidelně přehodnocována, aktualizována, případně revokována.

Článek 4

Pravidla pro ochranu zařízení

- (1) Technická aktiva informačních a komunikačních systémů (např. v serverovnách a ve vybraných datových pracovištích) jsou zabezpečena proti přístupu neautorizovaných osob a jsou situována do takových prostor, aby nedošlo k jejich odcizení.
- (2) Požadavky na ochranu zařízení k zabezpečení pracovišť UTB jsou stanoveny v jednotlivých provozních řádech, které jsou zpracovány pro každý objekt samostatně. Pokud se v nich nacházejí serverovny nebo datová pracoviště, jsou pro ně zpracovány řády zvlášť. Všechny provozní řády obsahují mimo jiné povolené přístupy a vlastníky privilegií ke správě zařízení.

Článek 5

Detekce narušení fyzické bezpečnosti

- (1) Narušení fyzické bezpečnosti je detekováno pracovníky fyzické ostrahy, popř. detekčním systémem napojeným na ústřednu PZTS. V případech, kdy narušení fyzické bezpečnosti detekují zaměstnanci UTB, je jejich povinností o této skutečnosti informovat pracovníky fyzické ostrahy, popř. Policii ČR. Postup na hlášení bezpečnostních incidentů je formálně popsán v provozním řádu daného objektu.
- (2) Monitorování prostor s technickými aktivy informačních a komunikačních systémů je v působnosti Technicko-provozního odboru (dále jen „TPO“), detekci jejich narušení musí bezodkladně oznámit jmenovanému správci daných prostor.

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