

Kód:	SR/29/2024	
Číslo jednací:	UTB/24/022964	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika bezpečného používání mobilních zařízení	
Organizační závaznost:	Univerzita Tomáše Bati ve Zlíně	
Datum vydání:	27.09.2024	Verze: 01
Účinnost:	01.10.2024	
Vydává:	Rektor	
Zpracoval:	Manažer kybernetické bezpečnosti	
Spolupracoval:	Centrum výpočetní techniky, Právní oddělení	
Počet stran:	4	
Počet příloh:	0	
Rozdělovník:	zaměstnanci UTB	
Podpis oprávněné osoby:	prof. Mgr. Milan Adámek, Ph.D., v.r.	

Článek 1 Úvodní ustanovení

- (1) Politika bezpečného používání mobilních zařízení jako součást *Deklarace kybernetické bezpečnosti Univerzity Tomáše Bati ve Zlíně* stanovuje pravidla pro používání mobilních zařízení ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“) a vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti“) v podmínkách Univerzity Tomáše Bati ve Zlíně (dále jen „UTB“).
- (2) Účelem této politiky je stanovit závazná pravidla a povinnosti pro nastavení mobilních zařízení využívaných k výkonu pracovních, studijních a dalších činností (dále jen „činností“) uživatelů na UTB. Uživatelé se rozumí:
 - a) studenti a zaměstnanci UTB, kteří mají zřízen uživatelský účet pro přístup do počítačové sítě UTB (dále jen „sít' UTB“),
 - b) hosté a další uživatelé využívajících sít' 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.
- (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 a postupy pro bezpečné používání mobilních zařízení

- (1) Mobilními zařízeními se rozumí veškerá mobilní zařízení umožňující zobrazování, editaci, ukládání, přenášení nebo tisk dat, tedy zejména:
 - a) notebook,
 - b) tablet, iPad a podobná přenosná zařízení,
 - c) chytrý telefon,
 - d) výměnný disk a paměťová karta používaná v těchto zařízeních,
 - e) flash paměť, digitální fotoaparát, MP3 přehrávač apod.
- (2) Používání mobilních zařízení pořízených a evidovaných v majetku UTB se řídí těmito bezpečnostními pravidly:
 - a) uživatel je povinen k výkonu svých činností používat mobilní zařízení, která mu byla přidělena UTB, a která splňují bezpečnostní požadavky UTB,
 - b) uživateli je zakázáno provádět vlastní modifikace a instalace aplikací na mobilním zařízení, veškeré instalace aplikací musí být prováděny pouze oprávněným zaměstnancem, zpravidla Správcem IT součástí v souladu s *Politikou organizační bezpečnosti*,
 - c) uživatel je povinen chránit mobilní zařízení před krádeží a zneužitím,
 - d) uživatel je povinen bezodkladně hlásit ztrátu mobilního zařízení,
 - e) uživatel nesmí umožnit přístup do mobilního zařízení neoprávněné osobě,
 - f) uživatel je povinen ve stanovených intervalech 1x měsíčně připojit mobilní zařízení uvedené v odst. 1, písm. a) až c) k síti UTB za účelem provedení aktualizací a kontrol,
 - g) uživatel nesmí měnit nastavená bezpečnostní pravidla na mobilním zařízení,
 - h) uživatel nesmí používat software, který byl Národním úřadem pro kybernetickou a informační bezpečnost označen jako bezpečnostní hrozba či zranitelnost,
 - i) výměnný disk, paměťová karta a flash paměť musí být šifrovány,
 - j) uživatel je povinen chránit přístup do mobilního zařízení uvedeného v odst. 1, písm. a) až c) heslem (včetně PIN) nebo gestem,
 - k) uživatel je povinen pro vzdálený přístup k vybraným informačním systémům a službám, databázím a aplikacím, využívat výhradně Virtual Private Network (VPN).
- (3) Používání soukromých mobilních zařízení k výkonu pracovních činností zaměstnance je zakázáno.
- (4) Používání všech ostatních mobilních zařízení se řídí těmito bezpečnostními pravidly:
 - a) instalace aplikací na mobilní zařízení nesmí ohrozit pořizované a zpracovávané informace v rámci významného informačního systému (dále jen „VIS“) UTB v souladu s *Politikou systému řízení bezpečnosti informací*,
 - b) uživatel je povinen chránit mobilní zařízení před krádeží a zneužitím,
 - c) uživatel je povinen bezodkladně hlásit ztrátu mobilního zařízení obsahující informace definované v písm. a),
 - d) uživatel nesmí umožnit jiné osobě přístup k mobilnímu zařízení, které obsahuje informace definované v písm. a),
 - e) uživatel je povinen chránit přístup do mobilního zařízení uvedeného v odst. 1, písm. a) až c) heslem (včetně PIN) nebo gestem.

- f) uživatel je povinen pro vzdálený přístup k vybraným informačním systémům a službám, databázím a aplikacím, využívat výhradně Virtual Private Network (VPN).

Článek 3

Pravidla pro připojování mobilních zařízení k síti UTB a povinnosti uživatelů

- (1) Následující pravidla se týkají mobilních zařízení specifikovaných v čl. 2, odst. 1, písm. a) až c) této směrnice, zpravidla tedy zařízení vybavených bezdrátovým síťovým komunikačním rozhraním.
- (2) V objektech UTB je umožněno uživatelům bezdrátové připojení k síti UTB prostřednictvím jejich mobilních zařízení.
- (3) Síť UTB je zapojena do mezinárodního projektu **eduroam** (www.eduroam.cz). Pro připojování mobilních zařízení uživatelů je primárně určena síť **eduroam**.
- (4) K síti **eduroam** se mohou uživatelé připojit s platnými přístupovými údaji, které jim poskytne jejich domovská organizace zapojená do projektu **eduroam**.
- (5) Aktuální informace o dostupnosti v jednotlivých lokalitách, způsobu a konfiguraci připojení, jsou uvedeny na adrese eduroam.utb.cz.
- (6) Pro speciální účely mohou být v rámci sítě UTB zřizovány bezdrátové sítě s dalšími názvy. Za zřizování těchto sítí zodpovídá Centrum výpočetní techniky (dále jen „CVT“) UTB.
- (7) Uživatelé sítě **eduroam** jsou povinni:
 - a) řídit se pravidly používání definovanými Roamingovou politikou federace eduroam.cz v platném znění (www.eduroam.cz),
 - b) dodržovat Podmínky přístupu k e-infrastruktuře CESNET (Access Policy – AP) v platném znění (www.cesnet.cz),
 - c) dodržovat ustanovení *Politiky bezpečnosti komunikační sítě*,
 - d) používat pouze přidělené přístupové údaje, za případné zneužití těchto přístupových údajů jsou uživatelé plně zodpovědní,
 - e) pro přidělení IP adresy používat DHCP protokol; nastavení statické IP adresy je závažným porušením této politiky,
 - f) neprodleně reagovat na výzvy a pokyny správy sítě hostující i domácí a roamingového centra sdružení CESNET, z. s. p. o.
- (8) Mobilní zařízení uživatelů musí vyhovovat platným normám a homologaci dle standardů IEEE 802.11 pro bezdrátový přístup a musí být odpovídajícím způsobem zabezpečena vhodnou konfigurací systému, aplikací bezpečnostních upgrade atd.
- (9) Na mobilních zařízeních je uživatelům zakázáno provozovat jakékoliv serverové aplikace a aplikace, které nepříznivě působí na provoz sítě nebo jejich služeb, nadměrně zatěžují síť nebo využívají její kapacitu.
- (10) Je zakázáno provozovat jiné bezdrátové sítě než písemně schválené CVT UTB.

- (11) V případě porušení těchto ustanovení, nebo nedostatečně zabezpečeného nebo zavírovaného mobilního zařízení, může správce sítě dočasně odejmout uživateli právo přístupu do sítě UTB. Případné další postihy vyplývající z ostatních předpisů nejsou tímto dotčeny.

Článek 4

Závěrečná ustanovení

- (1) Tato směrnice ruší a nahrazuje směrnici rektora č. 4/2016.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny
27.09.2024	01	Manažer KB	Vytvoření dokumentu