

Kód:	SR/22/2025	
Číslo jednací:	UTB/25/050857	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika bezpečného používání kryptografické ochrany	
Organizační závaznost:	Univerzita Tomáše Bati ve Zlíně	
Datum vydání:	08.09.2025	Verze: 01
Účinnost:	15.09.2025	
Vydává:	Rektor	
Zpracoval:	Manažer kybernetické bezpečnosti	
Spolupracoval:	Centrum výpočetní techniky, Právní oddělení, pověřenec OOÚ	
Počet stran:	3	
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 bezpečného používání kryptografické ochrany jako součást *Deklarace kybernetické bezpečnosti Univerzity Tomáše Bati ve Zlíně* stanovuje pravidla a postupy pro bezpečné používání kryptografické ochrany 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) Tato politika se vztahuje na všechny uživatele a informační aktiva, přičemž uživateli se rozumí studenti, zaměstnanci s uzavřenou pracovní smlouvou nebo dohodou o pracích konaných mimo pracovní poměr (dále jen „zaměstnanci UTB“), emeritní profesori a stipendisté na základě uzavřených dohod o spolupráci.
- (3) Přiměřeně se tato politika vztahuje i na zaměstnance významných dodavatelů a třetích stran na základě uzavřeného smluvního vztahu na dodávku služeb nebo produktů.
- (4) 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 Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu

- (1) Úroveň ochrany s využitím kryptografického algoritmu je dokumentována a řízena pro každé programové a technické vybavení podpůrného aktiva.

- (2) Na základě analýzy rizik primárních aktiv je stanovena požadovaná úroveň ochrany s přihlédnutím ke:
 - a) kategorizaci informací primárních aktiv,
 - b) použití přenosového média,
 - c) typu a síle kryptografického algoritmu.
- (3) Za dokumentování a řízení úrovně ochrany s využitím kryptografického algoritmu odpovídá Centrum výpočetní techniky (dále jen „CVT“).

Článek 3

Pravidla kryptografické ochrany informací

- (1) Pravidla pro použití kryptografické ochrany jsou dokumentována a řízena CVT.
- (2) Používány mohou být výhradně aktuálně odolné kryptografické algoritmy a kryptografické klíče.
- (3) Aktualizace kryptografických algoritmů je prováděna minimálně v souladu s platným doporučením Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“). Správci IT součástí mají povinnost při správě podpůrných aktiv tato doporučení dodržovat, což dokládají Garantovi primárního aktiva v záznamu kontrol, a to do konce roku, ve kterém ke změně došlo.
- (4) Pro vybraná aktiva jsou používána kryptografická opatření za účelem zajištění:
 - a) identifikačních a autentizačních prostředků,
 - b) autorizačních prostředků,
 - c) přenosu informací,
 - d) šifrování souborů,
 - e) zabezpečení elektronické pošty a přístupu k internetu.
- (5) Opatření kryptografické ochrany informací jsou implementována při přenosu po komunikační a datové síti (dále jen „sít' UTB“) a v souladu s *Politikou bezpečnosti komunikační sítě*:
 - a) při přístupu do vnitřní sítě UTB z vnějšího prostředí,
 - b) při výměně informací mezi systémy používanými v rámci činností UTB a externími subjekty.
- (6) Opatření kryptografické ochrany informací jsou implementována při ukládání souborů na mobilní zařízení nebo vyměnitelné nosiče dat pouze ve výjimečných případech a ve spolupráci s Garanty podpůrných aktiv, kteří vedou o těchto případech záznamy. Je použita jedna z těchto metod:
 - a) šifrování na úrovni celých disků,
 - b) šifrování na úrovni virtuálních disků,
 - c) šifrování na úrovni souborů.

- (7) Na ochranu elektronicky předávaných informací jsou použita opatření v souladu s *Politikou řízení aktiv* v platném znění a *Politikou bezpečného předávání a výměny informací* v platném znění. Předávání informací s externími subjekty (např. smluvními stranami) musí probíhat v souladu s *Politikou řízení dodavatelů* v platném znění.

Článek 4

Systém správy klíčů

- (1) Systém správy klíčů není ke dni vydání této směrnice v prostředí UTB implementován.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny
08.09.2025	01	Manažer KB	Vytvoření dokumentu