

Kód:	SR/14/2026	
Číslo jednací:	UTB/26/012224	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika zvládání kybernetických bezpečnostních incidentů	
Organizační závaznost:	Univerzita Tomáše Bati ve Zlíně	
Datum vydání:	23.02.2026	Verze: 01
Účinnost:	27.02.2026	
Vydává:	Rektor	
Zpracoval:	Manažer kybernetické bezpečnosti	
Spolupracoval:	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 zvládání kybernetických bezpečnostních incidentů jako součást *Deklarace kybernetické bezpečnosti Univerzity Tomáše Bati ve Zlíně* stanovuje postupy a odpovědnosti osob v případech zvládání kybernetického bezpečnostního incidentu 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 politiky je stanovit postupy vedoucí ke snížení dopadů kybernetických bezpečnostních incidentů a k zastavení jejich šíření a k prevenci před jejich opakováním.
- (3) Tato politika se vztahuje na všechny uživatele a informační aktiva. 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 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 Definování kategorií kybernetického bezpečnostního incidentu

- (1) Kategorie kybernetického bezpečnostního incidentu je dána úrovní jejich závažnosti a předpokládaného dopadu na aktiva UTB:

- a) kategorie „I“ – méně závažný incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy garantů aktiv nebo administrátorů k omezení dalšího šíření incidentu včetně minimalizace vzniklých škod,
 - b) kategorie „II“ – závažný incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy garantů aktiv nebo administrátorů k zabránění dalšího šíření incidentu včetně minimalizace vzniklých škod,
 - c) kategorie „III“ – velmi závažný incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy garantů aktiv nebo administrátorů k zabránění dalšího šíření incidentu včetně minimalizace vzniklých i potenciálních škod.
- (2) Pokud se nejedná o incident podle odstavce 1, jedná se o kybernetickou bezpečnostní událost.

Článek 3

Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů

- (1) Na UTB je zaveden nástroj pro detekci kybernetických bezpečnostních incidentů.
- (2) Na UTB je určen nástroj pro evidenci, správu a řešení provozních a bezpečnostních událostí a incidentů, který je jednotným kontaktním místem.
- (3) Na UTB jsou stanoveny postupy a role pro analýzu kybernetických bezpečnostních událostí, jejich kategorizaci a posouzení, zda se jedná o kybernetický bezpečnostní incident.
- (4) Postupy zvládání a kybernetických bezpečnostních incidentů jsou stanoveny v závislosti na hodnocení aktiv a rizik jednotlivých prvků informačních a komunikačních technologií.
- (5) V rámci klasifikace kybernetických bezpečnostních incidentů jsou posuzovány dopady, nutnost reakce a naléhavost řešení.
- (6) Forma a náležitosti hlášení kybernetických bezpečnostních incidentů Národnímu úřadu pro kybernetickou a informační bezpečnost (dále také „NÚKIB“) jsou stanoveny vyhláškou o kybernetické bezpečnosti.
- (7) Za nahlášení kybernetických bezpečnostních incidentů NÚKIB je na UTB odpovědný Manažer kybernetické bezpečnosti.

Článek 4

Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů

- (1) Testování systému zvládání kybernetických bezpečnostních incidentů je dokumentováno a řízeno.

- (2) Testování systému zvládání kybernetických bezpečnostních incidentů je prováděno jednou za rok.
- (3) K testování systému zvládání kybernetických bezpečnostních incidentů jsou použita pouze testovací data.

Článek 5

Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti

- (1) Každý kybernetický bezpečnostní incident je hodnocen z hlediska dopadů na důvěrnost, dostupnost a integritu jednotlivých aktiv.
- (2) Výsledky hodnocení kybernetického bezpečnostního incidentu jsou podnětem pro zlepšování kybernetické bezpečnosti.
- (3) Opatření plynoucí z vyhodnocení kybernetického bezpečnostního incidentu jsou podnětem pro aktualizaci Plánu zvládání rizik.
- (4) Každý kybernetický bezpečnostní incident, jeho vyhodnocení včetně návrhu na opatření jsou předkládána k projednání Výboru kybernetické bezpečnosti.

Článek 6

Hlášení a evidence událostí a incidentů

- (1) Evidence kybernetických bezpečnostních událostí a incidentů je na UTB centrálně vedena v nástroji pro evidenci, správu a řešení provozních a bezpečnostních událostí a incidentů.
- (2) V případě podezření či zjištění kybernetické bezpečnostní události nebo incidentu je uživatel povinen postupovat dle informací uvedených na webu UTB v sekci *Kybernetická bezpečnost*, konkrétně na webové stránce *Hlášení kybernetických událostí/incidentů* – <https://www.utb.cz/hlaseni-kybernetickych-udalosti-incidentu/>.
- (3) Za vedení evidence kybernetických bezpečnostních událostí a incidentů je odpovědný Ředitel Centra výpočetní techniky.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny
23.02.2026	01	Manažer KB	Vytvoření dokumentu