

Kód:	SR/36/2024	
Číslo jednací:	UTB/24/026133	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika řízení přístupů	
Organizační závaznost:	Univerzita Tomáše Bati ve Zlíně	
Datum vydání:	29.10.2024	Verze: 01
Účinnost:	01.11.2024	
Vydává:	Rektor	
Zpracoval:	Manažer kybernetické bezpečnosti	
Spolupracoval:	Centrum výpočetní techniky, Právní oddělení, pověřenec OOÚ	
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 řízení přístupů jako součást *Deklarace kybernetické bezpečnosti Univerzity Tomáše Bati ve Zlíně* stanovuje a rozpracovává požadavky na kybernetickou bezpečnost (dále jen „KB“) dle 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 pravidla pro přístup uživatelů k významnému informačnímu systému UTB (dále jen „VIS“), která určují postupy pro autorizaci, zřizování, změny a odebrání přístupových práv.
- (3) Tato politika se vztahuje na všechny zaměstnance UTB, informační aktiva vytvořená nebo používaná v rámci VIS, a na uživatele těchto aktiv.
- (4) Jednotlivé pojmy používané v této směrnici jsou vymezeny zejména zákonem o kybernetické bezpečnosti a vyhláškou o kybernetické bezpečnosti. Přehled jednotlivých pojmů je uveden v dokumentu *Pojmy kybernetické bezpečnosti*, který je dostupný na webu UTB v sekci *Kybernetická bezpečnost*.

Článek 2 Základní pravidla na řízení přístupů

- (1) Za stanovení základních pravidel v oblasti řízení přístupů je odpovědný Manažer kybernetické bezpečnosti (dále jen „Manažer KB“), za řízení přístupů odpovídá Garant primárního aktiva.
- (2) Garant primárního aktiva vede evidenci všech uživatelských účtů, pomocí které je možné jednoznačně identifikovat osobu používající daný uživatelský účet.

- (3) Přístupy a pokusy o přístup musí být automaticky zaznamenávány a monitorovány. Záznamy musí být uchovávány po dobu minimálně 6 měsíců.
- (4) Autentizační údaje nesmí být sdíleny více osobami.
- (5) Přidělování přístupových práv uživatelům a administrátorům se řídí následujícími pravidly:
- a) pro primární aktiva je proces přidělování řízený a dokumentovaný,
 - b) přidělování přístupových práv je prováděno pouze v rozsahu nutném pro výkon pracovních povinností a definuje se podle principu minima potřebného pro činnosti uživatele,
 - c) změna rozsahu přístupových oprávnění je řízena a schvalována na základě *Žádosti o přidělení/změnu přístupových práv*.
 - d) je vedena aktuální evidence všech uživatelských účtů pro primární aktiva a je definován systém uživatelských rolí a oprávnění, která schvaluje vedoucí zaměstnanec nebo gestor aktiva,
 - e) je vedena evidence o uskutečněných přístupech a o pokusech o přístup k primárnímu aktivu,
 - f) základním nástrojem pro řízení uživatelů je identity management,
 - g) k primárním aktivům je povolen přístup prostřednictvím propojení Virtual Private Network (VPN) nebo protokolu HTTPS,
 - h) vícefaktorová autentizace je využívána, pokud to umožňují technické podmínky jednotlivých primárních aktiv,
 - i) role uživatelů a administrátorů jsou odděleny,
 - j) postup řízení přístupů při mimořádných situacích je dokumentován Garantem primárního aktiva.

Článek 3

Požadavky na řízení přístupů

- (1) Systém řízení přístupů je tvořen:
- a) popisem rozsahu jednotlivých uživatelských rolí,
 - b) popisem požadavku na školení jednotlivých uživatelských rolí,
 - c) definicí kritické kombinace rolí,
 - d) popisem procesu přidělování uživatelských rolí,
 - e) popisem technologie ověření identity uživatelů,
 - f) popisem bezpečného chování uživatelů,
 - g) definicí životního cyklu přístupů uživatelů,
 - h) vynucováním pravidel pro ověření identity uživatelů.

Článek 4

Princip minimálních oprávnění/potřeba znát (need to know)

- (1) Každý uživatel má přístup pouze k těm aktivům, která nezbytně potřebuje k výkonu své práce.
- (2) Základní rozsah oprávnění k jednotlivým primárním aktivům je definován jako minimum potřebného pro činnosti, které uživatel potřebuje. Oprávnění jsou členěna do uživatelských rolí.

Článek 5

Životní cyklus řízení přístupů

- (1) Primární aktiva mají dokumentováno řízení přístupů, které probíhá ve fázích:
- a) žádost o přidělení přístupových práv,
 - b) schvalování a přidělení přístupových práv,
 - c) pravidelná kontrola přístupových práv,
 - d) změna přístupových práv,
 - e) zrušení přístupových práv.
- (2) V žádosti o přidělení přístupových práv jsou definovány minimálně tyto údaje:
- a) osoba oprávněna žádat,
 - b) uživatel,
 - c) rozsah oprávnění, případně zdůvodnění.
- (3) V procesu schvalování a přidělení přístupových práv jsou definovány minimálně tyto údaje:
- a) osoby oprávněné schválit požadavek,
 - b) osoby nastavující příslušná oprávnění.
- (4) V procesu změny přístupových práv jsou definovány minimálně tyto údaje:
- a) osoby oprávněné schválit požadavek,
 - b) osoby nastavující příslušná oprávnění.
- (5) Ke zrušení přístupových práv k informacím a primárním aktivům dochází:
- a) při změně pracovního zařazení nebo uživatelské role oznámením oprávněného vedoucího zaměstnance,
 - b) při ukončení pracovního nebo obdobného vztahu automaticky.
- (6) Systém řízení přístupů a stanovených pravidel pro řízení přístupů je pravidelně kontrolován Gestorem primárního aktiva.

Článek 6

Řízení privilegovaných oprávnění

- (1) Privilegovaným oprávněním se rozumí přístupové oprávnění k účtu, který ve VIS umožňuje nad rámec běžného uživatele vykonávat některou z uvedených činností:
- a) provádět změny v nastavení,
 - b) měnit rozsah přidělených oprávnění jednotlivých rolí a uživatelů,
 - c) vykonávat servisní činnosti bez přítomnosti uživatele.
- (2) Pro privilegované oprávnění je přiřazen odlišný identifikátor uživatele od běžně používaného uživatelského účtu.
- (3) Běžné činnosti nejsou prováděny s použitím privilegovaného oprávnění.

- (4) Přihlašovací relace musí mít nastavenou časově omezenou platnost bez ohledu na typ oprávnění uživatelského účtu, po jejím vypršení následuje automatické odhlášení od systému.

Článek 7

Řízení přístupů pro mimořádné situace

- (1) Za účelem zajištění kontinuity činnosti UTB během kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události nebo jiných mimořádných situací mohou být jednorázově nastavena přístupová oprávnění nad rámec standardního režimu provozu.
- (2) Procesy pro zvládání kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události nebo jiné mimořádné situace jsou definovány v havarijním plánu a zpracované pro každý VIS.

Článek 8

Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách

- (1) Proces pro přezkoumání přístupových oprávnění je definován v bezpečnostní dokumentaci zpracovávané pro primární aktiva.
- (2) Kontrolu přístupových oprávnění provádí Garant primárního aktiva, a to v celém rozsahu uživatelských oprávnění.
- (3) Dokumentace pro přezkoumání přístupových oprávnění obsahuje minimálně:
- a) stanovení cyklu provádění kontroly,
 - b) osoby provádějící kontrolu,
 - c) zápis o provedené kontrole,
 - d) postup nápravy při zjištění nedostatku.
- (4) Z přezkoumání přístupových oprávnění vypracuje Manažer KB zprávu, kterou schvaluje Výbor pro řízení kybernetické bezpečnosti UTB, který ji následně předkládá Vedení UTB.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny
29.10.2024	01	Manažer KB	Vytvoření dokumentu