

Kód:	SR/28/2024	
Číslo jednací:	UTB/24/022963	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika bezpečnosti lidských zdrojů	
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:	6	
Počet příloh:	2	
Rozdělovník:	zaměstnanci UTB	
Podpis oprávněné osoby:	prof. Mgr. Milan Adámek, Ph.D., v.r.	

Článek 1 Úvodní ustanovení

- (1) Politika bezpečnosti lidských zdrojů jako součást *Deklarace kybernetické bezpečnosti Univerzity Tomáše Bati ve Zlíně* stanovuje postupy a protokoly podporující účinnou správu aktiv 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 politiky je stanovit zásady a požadavky dopadající na zaměstnance UTB během jejich celého životního cyklu u zaměstnavatele počínaje nástupem, přes jeho výkon, případné změny a konče jeho odchodem v podmínkách UTB.
- (3) Tato politika se vztahuje na všechny zaměstnance UTB, informační aktiva vytvořená nebo používaná v rámci významného informačního systému (dále jen „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 Role a odpovědnosti

- (1) V popisech pracovních činností zaměstnanců jsou definovány pracovní role a odpovědnosti v oblasti bezpečnosti informací jejich přímým vedoucím zaměstnancem, a to v souladu se stanoveným vzorovým popisem práce pro garanty podpůrných aktiv schváleným

Výborem pro řízení kybernetické bezpečnosti. Role a odpovědnosti zaměstnanců v oblasti bezpečnosti informací jsou stanoveny a dokumentovány v souladu s *Politikou systému řízení bezpečnosti informací*.

- (2) Role a odpovědnosti v oblasti bezpečnosti informací zahrnují:
- a) požadavek na realizaci a dodržování zásad v souladu s bezpečnostní politikou informací,
 - b) požadavek na ochranu aktiv před neautorizovaným přístupem, vyzrazením, modifikací, zničením nebo narušením,
 - c) požadavek na vykonávání určitých bezpečnostních procesů nebo činností, legislativních zdrojů,
 - d) požadavek na určení jednoznačné odpovědnosti za provedené činnosti,
 - e) požadavek hlásit bezpečnostní události nebo jiná bezpečnostní rizika.
- (3) V rámci přijímacího pohovoru výběrového řízení jsou zájemcům o zaměstnání přímým vedoucím zaměstnancem nebo zaměstnancem vedoucím pohovor jasné sděleny role a odpovědnosti spojené s pracovní pozicí, o kterou se ucházejí.
- (4) Popisy pracovních činností jsou použity k doložení pracovních rolí a odpovědností v oblasti bezpečnosti informací.
- (5) Vedoucí zaměstnanci průběžně kontrolují uživatele, zda dodržují bezpečnost informací v souladu se zavedenými politikami a postupy.

Článek 3

Prověřování zaměstnanců

- (1) Všichni uchazeči o zaměstnání jsou prověřeni podle platných zákonů, interních předpisů a v souladu s etikou. Při prověření se zohledňují požadavky stanovené klasifikací informací, ke kterým by měl přijímaný zaměstnanec získat přístup, a také z hlediska jejich spolehlivosti a potenciálních rizik.
- (2) Při prověřování je brán zřetel na dodržení soukromí a ochranu osobních dat a požadavků souvisejících předpisů.
- (3) Pokud bude uchazeč o zaměstnání přijímán na pozici s přístupem k chráněným informacím, provede Personální oddělení prověření na základě:
- a) dostupnosti dostatečných referencí, například profesní a osobní,
 - b) ověření proklamovaného vzdělání a odborné kvalifikace,
 - c) ověření totožnosti,
 - d) popř. detailnějšího prověření (např. lustrační osvědčení, výpis z trestního rejstříku, u pozic s hmotnou odpovědností ověření v registru dlužníků atd.).

Článek 4

Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení

I. Způsoby a formy poučení uživatelů

- (1) Zaměstnanci, kterým bude umožněn přístup k citlivým informacím a prostředkům pro zpracování informací, budou nad rámec vstupního školení zaměstnanců svým přímým vedoucím zaměstnancem poučeni o pravidlech zajišťování bezpečnosti informací a podepíše dokument obsahující:
- a) práva a právní odpovědnost zaměstnanců v rolích uživatelů,
 - b) odpovědnosti zaměstnanců pro nakládání s informacemi obdrženými od jiných organizací a zúčastněných stran,
 - c) odpovědnosti UTB při nakládání s osobními údaji včetně těch údajů, které byly vytvořeny v průběhu pracovněprávního vztahu,
 - d) rozšíření odpovědností i mimo objekty UTB a mimo běžnou pracovní dobu (například v případě práce na dálku, na pracovní cestě apod.),
 - e) popis kroků, které budou následovat při nedodržení bezpečnostních požadavků ze strany zaměstnanců, a které jsou dány *Pracovním řádem UTB* v platném znění.

Podepsaný dokument, jehož vzor tvoří *Přílohu č. 1* této směrnice, je uložen v osobním spisu zaměstnance.

II. Způsoby a formy poučení garantů aktiv

- (2) Garanti aktiv budou Specialistou bezpečnosti IT v rámci jmenování do role garanta poučení o pravidlech zajišťování bezpečnosti informací a o pravidlech výkonu funkce garanta primárních/podpůrných aktiv, případně budou poučeni o specifických otázkách spojených s konkrétní skupinou aktiv. O provedeném poučení bude vyhotoven zápis, jehož vzor tvoří *Přílohu č. 2* této směrnice, podepsaný garantem aktiva.

III. Způsoby a formy poučení administrátorů

- (3) Administrátoři budou před svěřením konkrétních systémů či zařízení do správy svým přímým vedoucím zaměstnancem poučeni o pravidlech zajišťování bezpečnosti informací a o pravidlech výkonu funkce administrátora, případně budou poučeni o specifických otázkách spojených se spravovanými zařízeními. O provedeném poučení bude vyhotoven zápis, jehož vzor tvoří *Přílohu č. 2* této směrnice, zápis podepsaný administrátorem bude uložen v osobním spisu zaměstnance.

IV. Způsoby a formy poučení osob zastávajících bezpečnostní role

- (4) Osoby zastávající ostatní bezpečnostní role podle *Přílohy č. 6* vyhlášky o kybernetické bezpečnosti budou Manažerem kybernetické bezpečnosti (dále jen „Manažer KB“) v rámci jmenování do role poučeny o pravidlech zajišťování bezpečnosti informací a o pravidlech výkonu dané role, případně budou poučeny o specifických otázkách spojených s danou rolí. O provedení poučení bude vyhotoven zápis podepsaný osobu vykonávající bezpečnostní roli, formu zápisu stanoví Manažer KB.
- (5) Postup pro realizaci rozvoje bezpečnostního povědomí podrobně popisuje samostatný dokument *Plán rozvoje bezpečnostního povědomí*.

Článek 5

Bezpečnostní školení nových zaměstnanců

- (1) Každý nový zaměstnanec prochází úvodním bezpečnostním školením a poté, minimálně 1x za rok absolvuje pravidelné opakovací školení (se zohledněním případných změn v dokumentaci, postupech atd.).
- (2) Všichni zaměstnanci jsou pravidelně proškolení v souvislosti s bezpečností informací, a to v souladu s *Plánem rozvoje bezpečnostního povědomí* minimálně 1x za rok.
- (3) Používat prostředky informačních a komunikačních technologií může pouze zaměstnanec, který byl náležitě proškolen v oblasti bezpečnosti informací a s bezpečnostními opatřeními příslušnými jeho pracovnímu zařazení a absolvoval školení o práci v těch informačních systémech, které bude při výkonu svého zaměstnání využívat. O seznámení s uvedenými dokumenty a o školení musí být proveden zápis, který bude uložen v osobním spise zaměstnance.
- (4) V případě výskytu závažného kybernetického bezpečnostního incidentu jsou zaměstnanci mimořádně proškoleni.
- (5) Cílem bezpečnostního školení je především osvojení znalostí, jak předcházet bezpečnostním událostem a incidentům, jak se chovat v neobvyklých situacích a jak se z nich poučit. To znamená, že zaměstnanci:
 - a) porozumí své roli a budou si vědomi své zodpovědnosti vůči zaměstnavateli a okolí,
 - b) pochopí zásady systému řízení bezpečnosti informací a z nich vyplývající postupy,
 - c) se chovají v souladu se stanovenými bezpečnostními opatřeními,
 - d) budou mít znalosti o řídicích, provozních a technických mechanismech používaných k zajištění bezpečnosti aktiv, za které odpovídají anebo se kterými pracují.
- (6) Manažer KB zpracovává a vede o bezpečnostních školeních přehledy, které obsahují minimálně datum konání, předmět školení a seznam osob, které školení absolvovaly, a to včetně jejich podpisu v případě konání školení v prezenční formě.
- (7) Za provedení školení v oblasti bezpečnosti informací je odpovědný Manažer KB.

Článek 6

Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací

- (1) V případě výskytu závažného bezpečnostního incidentu, který byl způsoben porušením bezpečnostních politik UTB ze strany zaměstnanců, je vůči těmto zaměstnancům zahájen postup v souladu s příslušnými ustanoveními zákona č. 262/2006 Sb., zákoník práce v platném znění. Způsob řízení odpovídá povaze incidentu a jeho dopadu na UTB.
- (2) Při tomto porušení příslušný vedoucí zaměstnanec zohlední:
 - a) absolvování bezpečnostního školení,
 - b) povahu porušení bezpečnosti a jeho dopad,

- c) zda se jedná o první nebo opakované porušení,
 - d) zda se jedná o záměrné nebo nedbalostní porušení,
 - e) odpovídající legislativu,
 - f) existující smlouvy,
 - g) další relevantní okolnosti.
- (3) V případě podezření na spáchání trestného činu postupuje UTB v souladu s příslušnými ustanoveními trestního řádu a souvisejícími právními předpisy.

Článek 7

Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice

- (1) Při rozhodování o ukončení nebo změně pracovněprávního vztahu je odpovědný vedoucí zaměstnanec povinen zohlednit následující rizikové faktory:
- a) z jakých důvodů dochází ke změně nebo ukončení pracovněprávního vztahu,
 - b) stávající odpovědnosti zaměstnance,
 - c) hodnotu aktiv, ke kterým může mít (mohl mít) přístup.
- (2) Před ukončením nebo změnou pracovněprávního vztahu odpovědný vedoucí zaměstnanec odebere nebo omezí přístupová práva k informačním aktivům a prostředkům pro zpracování informací, nebo k tomu vydá písemný pokyn.
- (3) Pokud jsou přístupová práva sdílena mezi více zaměstnanci, rozhodne odpovědný vedoucí zaměstnanec o změně skupinových přístupových práv, tyto uživatele ze všech seznamů skupinových přístupových práv vyjme a všem ostatním zaměstnancům zakáže sdílet informace s odcházejícím zaměstnancem. Odpovědný vedoucí zaměstnanec o tomto postupu informuje správce aktiv.
- (4) V závažných případech je zaměstnanec okamžitě zbaven svých přístupových práv a výsad. Pokud hrozí pokračování v nepovolených event. zakázaných aktivitách, je zaměstnanec neprodleně vyveden z objektu UTB a je mu zakázán přístup na pracoviště.

I. Změna přístupových oprávnění při změně pracovní pozice

- (5) V případě změny pracovněprávního vztahu musí odpovědný vedoucí zaměstnanec kromě úpravy popisu práce vydat písemný pokyn ke změně přístupových oprávnění, a to jak v rovině fyzického přístupu (vstupní karty, klíče, aj.), tak především oprávnění k informačním systémům UTB tak, aby reflektovaly nové pracovní zařazení zaměstnance. Odpovědný vedoucí zaměstnanec o tomto vyhotoví formální zápis.

II. Vrácení svěřených aktiv a odebrání práv při ukončení pracovněprávního vztahu

- (6) V případě ukončení pracovněprávního vztahu musí zaměstnanec vrátit všechny zapůjčené prostředky, dokumenty a ostatní vybavení, vztahující se ke svěřeným aktivům. Odpovědné osoby za dané oblasti musí formálně potvrdit převzetí všech prostředků.
- (7) V případě ukončení pracovněprávního vztahu s klíčovými zaměstnanci (uživatelé s přidělenými rolemi ve VIS, garanti primárních aktiv, garanti podpůrných aktiv

v kategoriích technické vybavení, programové vybavení a komunikační prostředky) nebo zaměstnanci zastávajícími bezpečnostní role musí být zajištěno předání odpovědností.

- (8) Za proces a náležitosti spojené s ukončením pracovněprávního vztahu je odpovědný příslušný vedoucí zaměstnanec, který dbá na to, aby byly dodrženy všechny aspekty bezpečnosti a odpovídající postupy. V případech, kdy je to obsahem smlouvy, musí informovat zaměstnance, smluvní nebo třetí strany o provozních a personálních změnách.
- (9) V rámci procesu ukončování pracovněprávního vztahu odpovědný vedoucí zaměstnanec formálně potvrdí odebrání všech přístupových oprávnění odcházejícího zaměstnance, a to jak v rovině fyzického přístupu (vstupní karty, klíče, aj.), tak především oprávnění k informačním systémům UTB (zneplatnění všech přístupových oprávnění zaměstnance k datu ukončení pracovněprávního vztahu).

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