Kód:	SR/12/2024	
Číslo jednací:	UTB/24/007645	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika organizační bezpečnosti	
Organizační závaznost:	Univerzita Tomáše Bati ve Zlíně	
Datum vydání:	02.05.2024	Verze: 01
Účinnost:	03.05.2024	
Vydává:	Rektor	
Zpracoval:	Manažer kybernetické bezpečnosti	
Spolupracoval:	Centrum výpočetní techniky, Právní oddělení	
Počet stran:	6	
Počet příloh:	0	
Rozdělovník:	zaměstnanci UTB	
Podpis oprávněné osoby:	prof. Mgr. Milan Adámek, Ph.D., v.r.	

Článek 1
Úvodní ustanovení

(1) Politika organizační bezpečnosti jako součást *Deklarace kybernetické bezpečnosti Univerzity Tomáše Bati ve Zlíně* stanovuje bezpečnostní role a jejich odpovědnosti za prosazení a realizaci bezpečnostních opatření 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) Vzhledem ke skutečnosti, že UTB je správcem a provozovatelem významných informačních systémů (dále jen „VIS“), musí mít dle zákona o kybernetické bezpečnosti ustanovenu roli Manažera kybernetické bezpečnosti (dále jen „Manažer KB“) a Garanta primárního a podpůrného aktiva.

(3) Účelem této politiky je stanovit a popsat bezpečnostní role, které jsou součástí organizační struktury kybernetické bezpečnosti na UTB, a určit jejich povinnosti a odpovědnosti, definovat způsoby určení bezpečnostních rolí a popsat vzájemné vztahy jednotlivých bezpečnostních rolí.

(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
Bezpečnostní role, jejich práva a povinnosti

(1) Povinnost zřízení Výboru pro řízení kybernetické bezpečnosti (dále jen „Výbor KB“) a ustanovení Manažera KB, Architekta kybernetické bezpečnosti (dále jen „Architekt KB“), Garantů primárních a podpůrných aktiv a Auditora kybernetické bezpečnosti (dále jen „Auditor KB“) se řídí zákonem o kybernetické bezpečnosti a vyhláškou o kybernetické bezpečnosti.

(2) Bezpečností role jsou určeny příslušnými vnitřními normami UTB, a to, zejména *Statutem Výboru pro řízení kybernetické bezpečnosti*, *Statutem Manažera kybernetické bezpečnosti*, *Politikou řízení aktiv* a chráněným dokumentem *Hodnocení aktiv a rizik*.

(3) V případě nepřítomnosti zaměstnance, který zastává bezpečnostní roli na pracovišti, převezme výkon této bezpečností role zaměstnanec, dočasně k tomu pověřený příslušným nadřízeným zaměstnancem.

I. Výbor KB, jeho práva a povinnosti

(4) Výbor KB zajišťuje činnosti spojené s celkovým řízením a rozvojem VIS a významně se podílí na řízení a koordinaci činností spojených s kybernetickou bezpečností informačních systémů na UTB jako celku. Bližší působnost, pravomoci, odpovědnosti a složení členů Výboru KB jsou stanoveny *Statutem Výboru pro řízení kybernetické bezpečnosti*.

II. Manažer KB, jeho práva a povinnosti

(5) Manažer KB je bezpečnostní role odpovědná za plánování, organizování a řízení realizace opatření, projektů a programů k řízení bezpečnosti informací tak, aby bylo dosaženo cílů stanovených zákonem o kybernetické bezpečnosti a jeho prováděcími předpisy, a to ve stanoveném termínu a v rámci stanoveného rozpočtu. Role Manažera KB působí jako kontaktní osoba pro veškeré aspekty a otázky kybernetické bezpečnosti, která rovněž prosazuje a koordinuje úlohu systému řízení bezpečnosti informací (dále jen „SŘBI“) na UTB.

(6) Manažer KB je oprávněn navrhovat vedení UTB organizační opatření upravující činnosti obecně organizačního, administrativního nebo technického charakteru, včetně bezpečnostních aspektů.

(7) Klíčové činnosti, pravomoci a odpovědnosti Manažera KB jsou stanoveny ve *Statutu Manažera kybernetické bezpečnosti*.

III. Garant primárního aktiva, jeho práva a povinnosti

(8) Každé primární aktivum musí mít přiděleno svého Garanta primárního aktiva.

(9) Garant primárního aktiva je odpovědný za zajištění rozvoje, použití a bezpečnosti primárního aktiva (zajištění důvěrnosti, dostupnosti a integrity aktiva).

(10) Garant primárního aktiva:

a) poskytuje podklady Manažerovi KB za účelem provedení analýzy rizik pro dané primární aktivum,
b) ve spolupráci s Manažerem KB stanoví hodnotu aktiva z pohledu důvěrnosti, integrity a dostupnosti primárního aktiva,
c) stanovuje obecné bezpečnostní požadavky a koncepty (např. požadované doby obnovy, matici přístupu k primárnímu aktivu či další požadavky na bezpečné užívání, provoz a rozvoj) pro dané primární aktivum na základě klasifikace,
d) na základě návrhů Manažera KB, Garanta podpůrného aktiva či Správce IT součásti schvaluje navržená bezpečnostní pravidla a opatření řešící bezpečnostní požadavky pro dané primární aktivum, respektive související podpůrné aktivum typu aplikační služba,
e) zodpovídá za použití, rozvoj a bezpečnost aktiva,
f) informuje Manažera KB o všech změnách aktiva, které mají nebo mohou mít vliv na hodnotu aktiva.

IV. Garant podpůrného aktiva, jeho práva a povinnosti

(11) Každé podpůrné aktivum musí mít přiděleno svého Garanta podpůrného aktiva.

(12) Garant podpůrného aktiva je odpovědný za zajištění rozvoje, použití a bezpečnosti podpůrného aktiva (zajištění důvěrnosti, dostupnosti a integrity aktiva).

(13) Garant podpůrného aktiva:

a) provádí hodnocení důvěrnosti, integrity a dostupnosti podpůrného aktiva, a to na základě primárního aktiva či nadřazených technologických vrstev podpůrných aktiv, které dané aktivum podporuje,
b) v souladu s bezpečnostními požadavky a bezpečnostní dokumentací zajistí realizaci bezpečnostních opatření,
c) zajišťuje správu podpůrného aktiva a je odpovědný za jeho užívání v souladu s bezpečnostními požadavky a dokumentací a v souladu s přidělenou rolí,
d) informuje Manažera KB o všech změnách aktiva, které mají nebo mohou mít vliv na hodnotu podpůrného aktiva,
e) informuje Garanty příslušných podpůrných aktiv nadřazených technologických vrstev.

V. Správci IT součástí, jejich práva a povinnosti

(14) Správce IT součásti je výkonný zaměstnanec, který podle popisu práce zajišťuje minimálně jednu z níže uvedených činností:

a) instalaci, konfiguraci, správu, údržbu, a evidenci HW a SW, včetně koordinace servisu,
b) evidenci veškeré mu svěřené výpočetní techniky a komunikačních prostředků,
c) zálohování systémového programového vybavení a konfigurací a ochranu záložních médií,
d) správu a evidenci jím zpracované nebo mu svěřené technické a bezpečnostní dokumentace,
e) kontrolu auditních záznamů ve shodě s bezpečnostní dokumentací,
f) archivní kopie auditních záznamů (logů).

(15) Správce IT součásti zodpovídá za řízení, prosazování a kontrolu bezpečnosti informací v rámci svěřeného aktiva.

(16) Správce IT součásti udržuje aktuální seznam oprávněných uživatelů s jejich přidělenými přístupovými oprávněními.

(17) Správce IT součásti stanoví pravidla pro mazání dat a likvidaci technických nosičů dat v souladu s vyhláškou o kybernetické bezpečnosti.

(18) Správce IT součásti zajišťuje kontrolu dodržování zákonných a licenčních podmínek z hlediska využívání programového vybavení.

VI. Administrátor VIS, jeho práva a povinnosti

(19) Administrátor VIS zajišťuje správu, provoz, použití a bezpečnost technického aktiva.

(20) Administrátor VIS je odpovědný za realizaci bezpečnostních opatření v provozu VIS.

(21) Administrátor VIS vystupuje současně v roli Garanta příslušného aktiva, vykonává pokyny příslušného vedoucího zaměstnance a Gestora primárního aktiva.

Článek 3
Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí

(1) RACI matice bezpečnostních rolí kybernetické bezpečnosti (viz Tabulka č. 1) představuje vazby odpovědností rolí na jednotlivé oblasti SŘBI. Tyto vazby jsou reprezentovány písmeny R / A / C / I:

a) R (Responsible) – má odpovědnost za přímé provádění svěřeného úkolu,
b) A (Accountable) – má odpovědnost za to, že daný proces je vykonáván v souladu se schválenou podobou procesu,
c) C (Consulted) – spolupracuje na procesu,
d) I (Informed) – je informován o průběhu a výsledku jednotlivých fází procesu.

Oblast	ROLE					
	Výbor KB	**Manažer KB**	**Garant primárního aktiva**	**Garant podpůrného aktiva**	**Správce IT součásti**	**Administrátor VIS**
Řízení kybernetické bezpečnosti	**A**	**R**	**R**	**R**	**R**	**R**
Audit kybernetické bezpečnosti	**I**	**C / I**	**C / I**	**C / I**	**C/ I**	**C / I**
Návrh bezpečnostních opatření	**A**	**R**	**C**	**C**	**C**	**C**
Realizace bezpečnostních opatření	**I**	**A**	**R**	**R**	**A**	**R**
Zajištění rozvoje, použití a bezpečnosti primárního aktiva	**I**	**C**	**A**	**R**	**C**	**R**
Zajištění rozvoje, použití a bezpečnosti podpůrného aktiva	**I**	**C**	**C**	**A**	**C**	**R**

Tabulka č. 1: RACI matice bezpečnostních rolí kybernetické bezpečnosti

Článek 4
Požadavky na oddělení výkonu bezpečnostních a provozních rolí

(1) Povinnosti a vymezení působnosti jednotlivých rolí SŘBI musí být z důvodu střetu zájmů odděleny tak, aby se omezily příležitosti pro zneužití aktiv nebo jejich neoprávněné či neúmyslné změny.

(2) Role Manažera KB nejsou slučitelné s rolemi odpovědnými za provoz informačního a komunikačního systému a s dalšími provozními či řídicími rolemi.

(3) Správce IT součásti nesmí být Administrátor VIS, Garant stejného primárního aktiva, nebo Manažer KB.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny
02.05.2024	01	Manažer KB	Vytvoření dokumentu