Kód:	SR/40/2023	
Číslo jednací:	UTB/23/025920	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika systému řízení bezpečnosti informací	
Organizační závaznost:	Univerzita Tomáše Bati ve Zlíně	
Datum vydání:	27.11.2023	Verze: 01
Účinnost:	01.12.2023	
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 systému řízení bezpečnosti informací 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 nastínit strategické cíle Systému řízení bezpečnosti informací (dále jen „SŘBI“), rozsah a hranice SŘBI a další pravidla a postupy související s řízením SŘBI.

(3) 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
Cíle, principy a potřeby řízení bezpečnosti informací

(1) Cílem SŘBI je zajištění bezpečnosti informací (ve všech jejich formách a fázích zpracování) zpracovávaných ve významných informačních systémech (dále jen „VIS“) UTB za účelem plnění své funkce veřejné vysoké školy.

(2) Informace nesmí být dostupné nebo nesmí být odhaleny neautorizovaným jednotlivcům, entitám nebo procesům (princip důvěrnosti), musí být zajištěna jejich přesnost, úplnost (princip integrity) a musí být přístupné a použitelné na žádost autorizované entity (princip dostupnosti).

(3) Při zavádění SŘBI se berou v úvahu následující základní principy:

a) povědomí o potřebě řízení bezpečnosti informací,
b) přidělení odpovědnosti za bezpečnost informací,
c) začlenění závazku vedení UTB k řízení bezpečnosti informací,
d) posouzení rizik, které určuje vhodné kontrolní mechanismy k dosažení přijatelné úrovně rizik,
e) začlenění bezpečnosti jako základního prvku informačních sítí a systémů,
f) aktivní prevenci a odhalování incidentů v oblasti bezpečnosti informací,
g) zajištění komplexního přístupu k řízení bezpečnosti informací,
h) průběžné přehodnocování bezpečnosti informací a provádění případných úprav.

(4) Potřeby řízení bezpečnosti informací vyplývají z hodnocení aktiv a rizik. V rámci tohoto procesu jsou zhodnoceny hrozby, zranitelnosti a úrovně jednotlivých rizik. Následně jsou definována patřičná nápravná opatření.

(5) UTB musí prostřednictvím Výboru pro řízení kybernetické bezpečnosti (dále jen „Výbor KB“) a Manažera kybernetické bezpečnosti (dále jen „Manažer KB“) účinně snižovat rizika a s nimi spojené možné ztráty způsobené narušením důvěrnosti, integrity a dostupnosti informací, selháním zaměstnanců UTB a poškozením majetku.

Článek 3
Rozsah a hranice SŘBI

(1) Rozsah a hranice SŘBI jsou definovány objektovým perimetrem a logickým perimetrem. SŘBI se nevztahuje na systém řízení ochrany informací dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

(2) Do rozsahu SŘBI v podmínkách UTB patří v rámci VIS UTB následující oblasti:

a) všechny pořizované a zpracovávané informace,
b) všechny související procesy, lidské a materiální zdroje a příslušná dokumentace,
c) osobní údaje zaměstnanců UTB, studentů UTB, účastníků programů celoživotního vzdělávání UTB, uchazečů o studium na UTB a absolventů UTB,
d) prostory UTB,
e) zařízení a vybavení ve vlastnictví UTB,
f) informační a komunikační infrastruktura UTB,
g) uživatelé VIS UTB,
h) všichni dodavatelé (včetně subdodavatelů), kteří participují na dodávkách primárních a podpůrných aktiv i ve smyslu poskytovaných služeb.

Článek 4
Pravidla a postupy pro řízení dokumentace

(1) Řízení dokumentace a záznamů v podmínkách UTB probíhá s využitím standardních procesů spisové služby, správy dokumentů a organizačními pravidly. Za řízení procesu

dokumentace a záznamů kybernetické bezpečnosti odpovídá Manažer KB ve spolupráci s tajemníkem Výboru KB.

(2) Bezpečnostní dokumentace:

a) je tvořena dokumenty definovanými zákonem o kybernetické bezpečnosti a vyhláškou o kybernetické bezpečnosti,
b) musí být dostupná všem osobám vykonávajícím na UTB činnosti v oblasti KB,
c) je vedena ve spisové službě UTB.

(3) Při řízení bezpečnostní dokumentace jsou vytvářeny, prosazovány a dodržovány postupy pro:

a) schvalování dokumentů před jejich vydáním a kontrolu jejich správnosti,
b) aktualizaci dokumentů v případě potřeby včetně potvrzení jejich platnosti,
c) přezkoumávání dokumentů v pravidelných intervalech včetně potvrzení jejich platnosti,
d) zabezpečení označení změn a stavu po poslední revizi dokumentů,
e) zamezení neúmyslného použití neaktuálních dokumentů a jejich řádné označení, pokud vyvstala potřeba dokumenty uchovávat,
f) zajištění dostupnosti aktuálních verzí dokumentů,
g) zajištění čitelnosti a snadnou identifikaci dokumentů,
h) zajištění řízení včetně distribuce, řádného označení a oddělení dokumentace od jiných subjektů v rámci činnosti UTB,
i) zajištění principu minimálních oprávnění k dokumentům (need to know).

Článek 5
Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací

(1) V rámci přípravy strategie řízení KB budou definovány nároky na finanční i lidské zdroje nutné pro dosažení cílů informační bezpečnosti stanovených v rámci SŘBI. Manažer KB přednese tyto požadavky na zdroje v rámci schvalovacího procesu Výboru KB, ten je oprávněn schválit strategii KB pouze za předpokladu, že budou zajištěny odpovídající finanční a lidské zdroje pro její implementaci.

(2) Zdroje na rozvoj technických aspektů KB spravuje kvestor, zdroje na rozvoj lidských zdrojů, zejména na vzdělávání a školení uživatelů i odborných pracovníků budou alokovány v příslušných kapitolách rozpočtu s pevnou alokací na aktivity související s rozvojem informační a kybernetické bezpečnosti.

(3) Čerpání zdrojů alokovaných pro rozvoj KB podléhá předem schválení Výboru KB na UTB.

Článek 6
Pravidla a postupy pro provádění auditů kybernetické bezpečnosti

(1) Nezávislé audity stavu KB včetně plnění legislativních požadavků v této oblasti se provádí dle § 16 vyhlášky o kybernetické bezpečnosti v pravidelných intervalech alespoň každé 3 roky a při významných změnách.

(2) Audit KB musí být prováděn osobou vyhovující podmínkám stanoveným v § 7 odst. 4 vyhlášky o kybernetické bezpečnosti, která nezávisle hodnotí správnost a účinnost zavedených bezpečnostních opatření. Provádění auditu KB zajišťuje Auditor kybernetické bezpečnosti (dále jen „Auditor KB“), kterým může být zaměstnanec UTB, případně externí subjekt – právnická nebo fyzická osoba.

(3) Podrobné plánování a vyhodnocování auditu KB má v kompetenci Manažer KB společně s ředitelem CVT a řídí se Metodikou provádění auditu kybernetické bezpečnosti.

(4) V rámci auditu KB se:

a) provádí a dokumentuje dodržování bezpečnostní politiky včetně přezkoumání technické shody,
b) posuzuje soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy a normami, jinými předpisy a smluvními závazky vztahujícími se k VIS UTB a určí případná nápravná opatření pro zajištění souladu.

(5) Zpráva z auditu KB je předkládána Manažerovi KB a vedení UTB.

(6) Výsledky auditu se zohlední v Plánu rozvoje bezpečnostního povědomí a Plánu zvládání rizik.

Článek 7
Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací

(1) Přezkoumání SŘBI je prováděno alespoň 1x ročně a při významných změnách s cílem ověřit účelnost, efektivnost a adekvátnost zavedených bezpečnostních opatření provozovaného SŘBI formou interního auditu pod vedením Manažera KB, případně s využitím outsourcingu formou externí služby právnická nebo fyzická osoba.

(2) Vstupy do přezkoumání SŘBI tvoří:
a) vyhodnocená opatření z předchozího přezkoumání SŘBI,
b) identifikované změny a okolnosti, které mohou mít vliv na SŘBI,
c) zpětná vazba o výkonnosti SŘBI, především:
- neshody a nápravná opatření,
- výsledky monitorování a měření,
- výsledky předchozích auditů KB,
- naplnění cílů SŘBI,

d) výsledky hodnocení rizik a stav plnění plánu zvládání rizik,
e) výstupy ze skenování zranitelností a penetračního testování,
f) přehled kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů za uplynulé období,
g) vyhodnocení plánu vzdělávání v oblasti KB.

(3) Výstupy z přezkoumání obsahují:
h) identifikaci možností pro neustálé zlepšování,
i) doporučení potřebných rozhodnutí, stanovení nápravných opatření a osob zajišťujících výkon jednotlivých činností.

(4) Z přezkoumání SŘBI vypracuje Manažer KB zprávu, kterou schvaluje Výbor KB, který ji následně předkládá vedení UTB.

Článek 8
Posuzování kvality procesu řízení bezpečnosti

(1) Metrikami, které indikují kvalitu procesu řízení bezpečnosti jsou:

a) frekvence a rozsah kybernetických bezpečnostních událostí a incidentů, které měly za následek porušení důvěrnosti nebo integrity informací zpracovávaných ve VIS UTB,
b) frekvence a rozsah kybernetických bezpečnostních událostí a incidentů, které měly za následek porušení dostupnosti informací,
c) frekvence a rozsah případů poškození prestiže nebo dobrého jména UTB,
d) frekvence a rozsah případů porušení bezpečnostní politiky,
e) přítomnost koncepce bezpečnosti jako součást každého kroku a rozhodnutí při rozvoji VIS UTB,
f) obecné povědomí o principech bezpečnosti a konkrétní znalost bezpečnostní politiky u kompetentních pracovníků a jejich vnímání potřeby zajištění bezpečnosti.

Článek 9
Pravidla a postupy pro nápravná opatření a zlepšování SŘBI

(1) SŘBI je průběžně monitorován prostřednictvím nastavených procesů a prostředků (podle článků 5 a 6). SŘBI je udržován a zlepšován také prostřednictvím systému řízení neshod a incidentů.

(2) Veškerá nápravná opatření vychází ze zprávy z přezkoumání SŘBI. Nápravná opatření jsou projednána Výborem KB, k jednotlivým nápravným opatřením jsou stanoveny osoby odpovědné za zavedení nápravných opatření a dodržení termínu zavedení nápravného opatření.

(3) Na vzniklé neshody nebo incidenty navrhuje a realizuje nápravné opatření Manažer KB ve spolupráci s ředitelem CVT. V rámci proaktivního přístupu implementuje Manažer KB také preventivní opatření, jejichž úkolem je vylepšit SŘBI.

(4) Nápravná opatření jsou pololetně sledována v rámci schůzí Výboru KB.

Článek 10
Klasifikace a přístup k informacím

(1) Klasifikace informací je nástrojem pro zajištění přiměřenosti ochrany informačních aktiv UTB. Na základě stanovených pravidel jsou informace rozdělovány a jsou stanovovány požadavky na jejich ochranu. Klasifikace informací poskytuje uživatelům informaci o nutnosti zvláštního zacházení s nimi.

(2) Klasifikace informací a jí odpovídající bezpečnostní opatření musí brát ohled na potřeby UTB, na sdílení informací nebo omezování přístupu k nim, a především na výši potencionálních negativních dopadů při narušení jejich bezpečnosti.

(3) Informace a výstupy ze systémů, které zpracovávají klasifikované informace, musí být označovány v souladu s jejich hodnotou a citlivostí.

(4) Při vzniku informace, resp. při přijetí informace od třetích stran, zaměstnanec, který informaci přijal, rozhoduje, zda informace vyžaduje zvláštní ochranu na základě posouzení kritičnosti informace.

(5) Klasifikační schéma přístupu k informacím určuje tyto stupně klasifikace informací:

a) **Veřejné** – informace, které jsou přístupné všem zaměstnancům UTB, studentům UTB i veřejnosti a jsou schváleny vlastníkem ke zveřejnění. Informace nevyžadují zvláštní úroveň ochrany z pohledu důvěrnosti. Je však nutné dbát na jejich ochranu z pohledu integrity, aby nedošlo ke zveřejnění informací, které neodpovídají skutečnosti. Přístup k veřejným informacím nesmí být omezován.
b) **Interní** – informace, které jsou určeny pro interní použití všem zaměstnancům UTB, studentům UTB nebo vybrané skupině, avšak nikoli skrze veřejně dostupné kanály. Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, které jsou vázány příslušnými dohodami o mlčenlivosti a tyto informace potřebují ke splnění smluvní závazků. Příjemce musí při předání nastavit důvěrnost komunikace, která zajistí odpovídající ochranu při přenosu a ukládání.
c) **Chráněné** – informace nejsou veřejně přístupné a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními. Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny
27. 11.2023	01	Manažer KB	Vytvoření dokumentu