Kód:	SR/41/2023	
Číslo jednací:	UTB/23/025921	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika řízení aktiv	
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:	7	
Počet příloh:	1	
Rozdělovník:	zaměstnanci UTB	
Podpis oprávněné osoby:	prof. Mgr. Milan Adámek, Ph.D., v.r.	

Článek 1
Úvodní ustanovení

(1) Politika řízení aktiv 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“) pro podmínky Univerzity Tomáše Bati ve Zlíně (dále jen „UTB“).

(2) Účelem politiky je nastínit strategické cíle a postupy řízení aktiv se zaměřením na primární a podpůrná aktiva významných informačních systémů (dále jen „VIS“) v podmínkách UTB.

(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
Identifikace primárních aktiv

(1) Manažer kybernetické bezpečnosti (dále jen „Manažer KB“) ve spolupráci s vedoucími zaměstnanci UTB identifikuje primární aktiva v agendách UTB.

(2) Primární aktiva jsou jedinečná, vycházející z klíčových procesů a činností důležitých pro provoz VIS na UTB. Při jejich identifikaci se vychází z dokumentů např.:

a) Statutu UTB,
b) Organizačního řádu rektorátu UTB,
c) vnitřních předpisů a norem,
d) legislativních zdrojů,
e) dokumentů a publikací NÚKIB,
f) interních aktů řízení organizace atd.

(3) Primární aktivum je jedno ze tří typů:

a) systém,
b) informace/agenda,
c) služba.

(4) Manažer KB na základě identifikace primárních aktiv navrhne u každého aktiva, zda patří do SŘBI.

(5) Každé jednotlivé primární aktivum musí mít přiřazeno Gestora aktiva a Garanta primárního aktiva, oba musí být uvedeni v Hodnocení aktiv a rizik, které je chráněným dokumentem. Přístup k Hodnocení aktiv a rizik nebo jeho částem je omezen obvykle na členy Výboru pro řízení kybernetické bezpečnosti (dále jen „Výbor KB“), gestory, garanty a jejich vedoucí zaměstnance.

(6) Jednotlivé Gestory primárních aktiv a Garanty primárních aktiv určuje Manažer KB ve spolupráci s vedoucími zaměstnanci UTB.

(7) Manažer KB předloží Výboru KB k projednání návrh na určení Gestorů aktiv a Garantů primárních aktiv.

Článek 3
Hodnocení primárních aktiv

(1) Hodnocení identifikovaných primárních aktiv je řízeno a dokumentováno v Hodnocení aktiv a rizik, které je chráněným dokumentem s omezeným přístupem.

(2) Hodnocení primárních aktiv provede Gestor aktiva a Garant primárního aktiva ve spolupráci s Manažerem KB.

(3) Hodnocení důležitosti primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti je provedeno na stupnicích dle tabulek, které jsou uvedeny v Metodice pro identifikaci a hodnocení aktiv a pro hodnocení rizik.

Článek 4
Evidence primárních aktiv

(1) Primární aktiva musí být evidována ve vhodném systému evidence aktiv a evidence musí obsahovat podrobné údaje, zejména:

a) ID,
b) typové primární aktivum,
c) název,
d) kategorie,
e) specifikace,
f) gestor aktiva,
g) garant primárního aktiva,
h) osobní údaje,
i) legislativa,
j) hodnocení aktiva z hlediska důležitosti (dostupnost, důvěrnost, integrita),
k) hodnota aktiva,
l) další informace o aktivu – např. určený informační systém a rozsah SŘBI.

(2) Manažer KB a Garant primárního aktiva jsou odpovědní za vedení centrální evidence primárních aktiv v elektronické podobě.

(3) Evidence primárních aktiv je vedena v Hodnocení aktiv a rizik.

Článek 5
Identifikace podpůrných aktiv

(1) Manažer KB identifikuje ve spolupráci s Garantem primárního aktiva a vedoucími zaměstnanci UTB podpůrná aktiva v agendách UTB.

(2) Podpůrná aktiva zajišťují existenci primárních aktiv a mohou být společná pro více primárních aktiv.

(3) Při identifikaci podpůrných aktiv je nutné vycházet z architektury systému a potřeby pro funkčnost primárního aktiva.

(4) Podpůrné aktivum je jedno že šesti typů:

a) HW – technické vybavení,
b) SW – programové vybavení,
c) objekty – prostory, budovy,
d) komunikační prostředky – infrastruktura,
e) lidské zdroje,
f) dodavatelé,
g) externí systémy a služby.

(5) Každé jednotlivé podpůrné aktivum musí mít přiřazeno Garanta podpůrného aktiva. který musí být uveden v Hodnocení aktiv a rizik.

(6) Role Garanta podpůrného aktiva může být totožná s rolí správce podpůrného aktiva.

(7) Jednotlivé Garanty podpůrných aktiv určuje ředitel Centra výpočetní techniky ve spolupráci s Manažerem KB, Garanty primárních aktiv a vedoucími útvarů zaměstnanců, kteří mají za podpůrná aktiva odpovědnost.

(8) Manažer KB předloží Výboru KB k projednání návrh na určení Garantů podpůrných aktiv.

Článek 6
Hodnocení podpůrných aktiv

(1) Hodnocení identifikovaných podpůrných aktiv je řízeno a dokumentováno v Hodnocení aktiv a rizik.

(2) Hodnocení provede Garant primárního aktiva a Garant podpůrného aktiva ve spolupráci s Manažerem KB.

(3) Při hodnocení podpůrných aktiv se zohlední vazby mezi podpůrnými a primárními aktivy následovně:

a) varianta A: podpůrná aktiva dědí hodnoty primárních aktiv,
b) varianta B: podpůrná aktiva jsou posuzována individuálně s ohledem na hodnotu primárních aktiv,
c) varianta C: podpůrná aktiva přebírají hodnoty primárních aktiv prostřednictvím vzorce.

(4) Hodnocení podpůrných aktiv musí být v souladu s hodnocením primárních aktiv a hodnotí se minimálně z pohledu důvěrnosti, integrity a dostupnosti na stupnicích dle tabulek, které jsou uvedeny v Metodice pro identifikaci a hodnocení aktiv a pro hodnocení rizik.

Článek 7
Evidence podpůrných aktiv

(1) Podpůrná aktiva musí být evidována ve vhodném systému evidence aktiv a evidence musí obsahovat podrobné údaje, zejména:

a) ID,
b) kategorie podpůrného aktiva,
c) skupina podpůrného aktiva,
d) typové podpůrné aktivum,
e) název,
f) popis podpůrného aktiva,
g) gestor aktiva,
h) garant podpůrného aktiva.
i) hodnocení aktiva z hlediska důvěrnosti, integrity, dostupnosti,
j) další relevantní informace o aktivu – např. jakého mají provozovatele, zda se jedná o významného dodavatele, zda jde o určený informační systém a rozsah SŘBI.

(2) Manažer KB a Garant podpůrného aktiva jsou odpovědní za vedení centrální evidence podpůrných aktiv v elektronické podobě.

(3) Evidence podpůrných aktiv je vedena v Hodnocení aktiv a rizik.

Článek 8
Určení vazeb mezi primárními a podpůrnými aktivy

(1) Vazby určené mezi primárními a podpůrnými aktivy jsou součástí Hodnocení aktiv a rizik.

(2) Pro analýzu a dokumentaci vlastností, závislostí a složení všech aktiv jsou klíčové pohovory Gestora aktiva, Garanta primárního aktiva, Garanta podpůrného aktiva a vedoucích zaměstnanců odborných oddělení ve spolupráci s Manažerem KB.

Článek 9
Pravidla ochrany jednotlivých úrovní aktiv

(1) Podle zákona o kybernetické bezpečnosti jsou stanovena:

a) pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv:
   - určením způsobů rozlišování jednotlivých úrovní aktiv,
   - stanovením pravidel pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv a
   - stanovením přípustných způsobů používání aktiv,

b) pravidla ochrany odpovídající úrovni aktiv a
c) způsoby pro spolehlivé smazání nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv.

(2) Aktiva jsou označována v souladu s nastavenými pravidly podle jejich klasifikace.

(3) Pravidla ochrany jednotlivých úrovní aktiv jsou odvozena od úrovně hodnocení důvěrnosti, integrity a dostupnosti.

(4) Na základě hodnocení aktiv jsou určeny možné způsoby zacházení s jednotlivými aktivy, které obsahují informace a stanoveny možné způsoby likvidace dat pro jednotlivé úrovně aktiv. Způsoby zacházení s jednotlivými aktivy musí být zvoleny přiměřeně k jednotlivým úrovním aktiv. Klasifikaci informací musí provést odpovědný garant primárního aktiva, garant podpůrného aktiva nebo autor informace. Úroveň aktiva ovlivní sdílení informací o aktivu.

(5) Pravidla ochrany aktiv, včetně způsobů rozlišování jednotlivých úrovní aktiv, pravidel pro manipulaci a evidenci aktiv podle úrovní aktiv a přípustné způsoby používání aktiv jsou uvedeny v Klasifikaci aktiv včetně zacházení s aktivy, která je Přílohou č. 1.

(6) Definovaná pravidla pro přijatelné použití aktiv se vztahují na všechny uživatele aktiv, dodavatele a třetí strany a musí být zdokumentována.

(7) Všichni zaměstnanci UTB a externí pracovníci jsou povinni se seznámit s klasifikací informací a pravidly pro zacházení s chráněnými informacemi a podle toho s informacemi dále pracovat.

Článek 10
Způsoby likvidace dat

(1) Pravidla pro mazání dat a likvidaci technických nosičů dat jsou definována v souladu s vyhláškou o kybernetické bezpečnosti a musí nabízet přiměřená bezpečnostní opatření s ohledem na hodnotu a důležitosti aktiv.

(2) Pravidla pro likvidaci dat jsou stanovena přiměřeně hodnotě a důležitosti aktiv a zohledňují:

a) hodnotu aktiva (zejména z pohledu důvěrnosti),
b) technologii (typy a velikost nosičů informace),
c) zda se nosič informace nachází pod kontrolou organizace či nikoliv,
d) zda jsou data součástí dedikovaného nebo multitenantního prostředí,
e) kdo bude likvidaci dat provádět (interní zaměstnanec, nebo dodavatel),
f) dostupnost vybavení a nástrojů pro likvidaci,
g) kapacitu likvidovaných nosičů,
h) zda je k dispozici vyškolený personál,
i) časovou náročnost likvidace,
j) cenu likvidace s ohledem na nástroje, školení, validaci, opětovné využití nosiče informace,
k) možné způsoby likvidace dat (například zničením nosiče, několikanásobným přepsáním nosiče dat, znečitelněním dat jejich šifrováním a podobně),
l) použitelné způsoby likvidace dat vzhledem ke stavu nosiče informace (například při poškození zařízení nebude možné použít variantu přepisu informace, ale některý ze způsobů fyzické likvidace).

(3) Způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií jsou následující:

a) Odstranění:
- odstranění dat tak, aby byla pro systém nedostupná (odstranění datového souboru, vyhození výtisku do odpadu),
- jde o nejméně bezpečný způsob likvidace dat, informace lze obnovit,
- není použitelné pro nosiče neumožňující opětovný zápis,
- použitelný způsob pro úroveň důvěrnosti aktiva: nízká.

b) Přepsání:
- přepsání chráněné informace nahodilými hodnotami,
- jde o středně bezpečný způsob likvidace dat, volně dostupné nástroje neumožňují obnovení informace,
- může být nahrazeno nebo kombinováno bezpečnou likvidací kryptografických klíčů k zašifrované informaci,
- není vhodné pro poškozená média, média neumožňující opětovný zápis nebo média s velkou kapacitou,
- použitelný způsob pro úroveň důvěrnosti aktiva: nízká až kritická.

c) Fyzická likvidace nosiče informace:
- zničení nosiče informace, příp. rozebrání zařízení a zničení nosiče informace, skartace výtisků,

- nejbezpečnější metoda likvidace dat, nosič informace nelze znovu použít, původní informace nelze znovu obnovit,
- použitelný způsob pro úroveň důvěrnosti aktiva: střední až kritická.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny
27.11.2023	01	Manažer KB	Vytvoření dokumentu