

Kód:	SR/7/2023	
Druh:	SMĚRNICE REKTORA	
Číslo jednací:	UTB/23/005941	
Klasifikace dokumentu:	INTERNÍ	
Název:	Statut Manažera kybernetické bezpečnosti	
Organizační závaznost:	Univerzita Tomáše Bati ve Zlíně	
Datum vydání:	30. 3. 2023	Verze: 01
Účinnost od:	3. 4. 2023	
Vydává:	Rektor	
Zpracoval:	Centrum výpočetní techniky	
Spolupracoval:	Právní oddělení	
Počet stran:	5	
Počet příloh:	0	
Rozdělovník:	zaměstnanci UTB	
Podpis oprávněné osoby:	prof. Mgr. Milan Adámek, Ph. D., v. r.	

Článek 1 Úvodní ustanovení

- (1) Manažer kybernetické bezpečnosti (dále jen „Manažer KB“ a kybernetická bezpečnost dále jen „KB“) Univerzity Tomáše Bati ve Zlíně (dále jen „UTB“) zajišťuje úkony vyplývající z povinností role manažera kybernetické bezpečnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), 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“).
- (2) Pozice Manažera KB UTB může být vykonávána zaměstnancem UTB, případně zajišťována prostřednictvím externího subjektu – fyzické nebo právnické osoby.
- (3) Manažer KB je podřízen rektorovi UTB a při plnění své funkce se řídí jeho pokyny v souladu s požadavky právních předpisů a interních norem v podmínkách UTB.
- (4) Manažer KB je pověřen komunikovat s regulačními orgány v oblasti kybernetické a informační bezpečnosti, zejména s NÚKIB a s GovCERT.CZ/CSIRT.CZ.

Článek 2 Základní pojmy

Aktiva

Primární aktiva jsou informace nebo služby, které zpracovává nebo poskytuje informační a komunikační systém.

Podpůrná aktiva jsou technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému.

Technickými aktivy jsou technické vybavení, komunikační prostředky a programové vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad na informační a komunikační systém.

Garant primárního aktiva je nejčastěji zaměstnanec zastávající role typu vedoucí oddělení, vedoucí odboru, vlastník procesu, vlastník systému atd.

Garant podpůrného aktiva je vybírán na základě jeho pracovního zařazení, procesních a odborných znalostí daného aktiva. Musí být schopen na základě možných dopadů ohodnotit aktivum tak, aby byla osoba odpovědná za zpracování hodnocení rizik schopna tato rizika adekvátně vyhodnotit a řídit.

Bezpečnostní týmy hrají klíčovou roli při ochraně kritické informační infrastruktury a významných informačních systémů podle zákona o kybernetické bezpečnosti a jeho prováděcích předpisů. Úlohou těchto týmů je zároveň působit jako prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace i občany.

GovCERT.CZ je vládní tým Národního centra kybernetické bezpečnosti, k jeho hlavním činnostem patří řešení bezpečnostních incidentů, zejména konzultacemi a poskytováním služeb analýzy síťových dat a logů s cílem identifikace způsobu a důsledků incidentu.

CSIRT je celosvětově používaná zkratka z anglického názvu Computer Security Incident Response Team.

CSIRT.CZ je národní CSIRT tým České republiky, který je provozován sdružením CZ.NIC podle zákona o kybernetické bezpečnosti a veřejnoprávní smlouvy uzavřené s Národním bezpečnostním úřadem.

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) je ústředním správním úřadem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.

Systém řízení bezpečnosti informací (dále jen „SŘBI“) je dokumentovaný systém, ve kterém jsou chráněna definovaná informační aktiva, jsou řízena rizika bezpečnosti informací a zavedená opatření jsou kontrolována. Při zavádění v organizaci se postupuje podle normy ISO/IEC 27001.

Update označuje aktualizaci systému, při které je upravena či doplněna verze stávající. Aktualizace se provádí z důvodu implementace vyšší bezpečnosti nebo opravy chyb.

Upgrade označuje výměnu aktuální verze systému za novou, příp. vyšší verzi.

Článek 3

Práva a povinnosti Manažera KB

- (1) Manažer KB odpovídá za prosazování a řízení realizace kybernetických a informačních bezpečnostních projektů a programů schválených Výborem KB na základě pokynů rektora UTB tak, aby informační a komunikační infrastruktura UTB poskytovala služby v této oblasti v souladu s aktuální právní úpravou v oblasti kybernetické a informační bezpečnosti.

- (2) Manažer KB odpovídá za tvorbu, prosazování a zajišťování SŘBI od průzkumu a analýz, přes průběžné testování prevence až po eliminaci následků a vyhodnocení kybernetických incidentů na UTB.
- (3) Manažer KB odpovídá za tvorbu, prosazování a zajišťování aktualizace vnitřních norem v oblasti KB.
- (4) Manažer KB spolupracuje při identifikaci aktuálního rozsahu a úplnosti informací o aktivech, identifikaci zdrojů, a návrhu na způsoby doplnění chybějících informací.
- (5) Manažer KB odpovídá za zajištění schopnosti UTB implementovat bezpečnostní opatření (organizační a technická) ukládaná zákonem o kybernetické bezpečnosti a za včasnou a hospodárnou implementaci těchto opatření.
- (6) Manažer KB průběžně analyzuje vývoj SŘBI a vyhodnocuje identifikovaná kybernetická rizika, detekované kybernetické bezpečnostní události a odhalené kybernetické incidenty a předkládá o tom zprávu, jejímž obsahem jsou i návrhy na zmírnění nepřijatelných rizik a návrhy na změnu priorit bezpečnostních projektů, a to pravidelně každé pololetí Výboru KB.
- (7) Manažer KB je oprávněn stanovit:
 - a) rozsah a hranice SŘBI (s ohledem na aktiva a organizační bezpečnost), ve kterém určí, kterých organizačních částí a technických prvků se SŘBI týká,
 - b) jednotnou metodiku pro identifikaci a hodnocení aktiv a metodiku pro stanovení kritérií pro přijatelnost rizik,
 - c) cíle kontinuity činností a strategii (plán) řízení kontinuity další činnosti včetně standardizace procesů pro oblast kybernetické a informační bezpečnosti,
 - d) provozní pravidla a postupy SŘBI,
 - e) Plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik včetně určení osoby zajišťující prosazování bezpečnostních opatření.
- (8) Manažer KB spolupracuje při schvalování závazných norem pro výběr, unifikaci a systemizaci technických a programových prostředků informačních technologií v podmínkách UTB.
- (9) V případě projektů týkajících se informačních systémů, obvykle při implementaci nového nebo update/upgrade již provozovaného systému Manažer KB:
 - a) konzultuje organizaci kontrol etap dílčího plnění,
 - b) rozhoduje se systémovým integrátorem o přípravě testovacích dat a organizaci bezpečnostního testování,
 - c) je informován o zkušebním a ověřovacím provozu a zátěžových testech,
 - d) podílí se na přípravě a organizaci akceptačního řízení.
- (10) Manažer KB kontroluje po věcné stránce formulaci zadávacích podmínek veřejných zakázek (včetně veřejných zakázek malého rozsahu) na výstavbu a modernizaci informačních a komunikačních systémů UTB či na pořízení dodávek či služeb, jejichž komponenty mohou mít vliv na KB UTB, z hlediska standardů kybernetické bezpečnosti a poskytuje součinnost zadavateli v zadávacích řízeních týkající se vyřešení otázek

souvisejících s KB; podrobnější úprava je případně stanovena v samostatných vnitřních normách UTB.

- (11) Manažer KB spolupracuje při procesu řízení rizik, jejich rozsahu a dopadu.
- (12) Manažer KB koordinuje řízení kybernetických incidentů.
- (13) Manažer KB předkládá návrh na realizaci bezpečnostního opatření Výboru KB k posouzení. Výbor KB po projednání doporučí rektorovi ke schválení realizaci bezpečnostního opatření. Podkladem jsou informace z monitorovacích a dohledových systémů, odborné stanovisko manažera KB a případné pokyny nebo rozhodnutí NÚKIB.
- (14) Manažer KB zajišťuje:
 - a) detekci kybernetických bezpečnostních událostí,
 - b) zpracovávání Zpráv o hodnocení aktiv a rizik, Plán zvládání rizik a Prohlášení o aplikovatelnosti, které předkládá Výboru KB,
 - c) u dodavatelů pravidelné hodnocení rizik, provádění kontrol zavedených bezpečnostních opatření u poskytovaných služeb a odstraňování zjištěných nedostatků,
 - d) aktualizaci SŘBI a příslušné dokumentace dle výsledků auditů nebo významných změn a vyhodnocení vhodnosti a účinnosti bezpečnostních opatření,
 - e) aktualizaci Zprávy o hodnocení aktiv a rizik, Bezpečnostní politiky, Plánu zvládání rizik a Plánu rozvoje bezpečnostního povědomí,
 - f) přípravu podkladů pro realizaci reaktivních opatření vydaných NÚKIB a pro realizaci bezpečnostních opatření (organizační a technická),
 - g) součinnost při provádění kontrolních auditů KB prováděných NÚKIB a jejich analýze.
- (15) Manažer KB vypracovává Plán rozvoje bezpečnostního povědomí a s tímto plánem seznamuje Výbor KB.
- (16) Manažer KB koordinuje opatření ke zvýšení bezpečnostního povědomí v podmínkách UTB včetně školení v oblasti kybernetické a informační bezpečnosti.
- (17) Manažer KB dohlíží na stanovení pravidel pro dodavatele (poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti informačních a komunikačních technologií), z pohledu plnění požadavků zákona o kybernetické bezpečnosti a prováděcích předpisů.
- (18) Manažer KB provádí pravidelný reporting pro vedení UTB o aktuálním stavu SŘBI, bezpečnostních incidentech, zjištěných neshodách a nedostatečné efektivnosti bezpečnostních opatření.
- (19) Manažer KB pravidelně komunikuje s vedením UTB.

Článek 4 **Kompetence Manažera KB**

- (1) Manažer KB je oprávněn vyžadovat od Výboru KB vyjádření a stanoviska o:

- a) přijatelnosti či nepřijatelnosti identifikovaných kybernetických bezpečnostních rizik včetně stanovení ještě přijatelné míry rizika a stanovení limitu finančních prostředků na eliminaci nepřijatelných rizik,
- b) prioritách realizace bezpečnostních opatření a navržených bezpečnostních projektů,
- c) určení osob pro výkon rolí garantů aktiv,
- d) provedení základní identifikace aktiv.

(2) Manažer KB je oprávněn vyžadovat od garantů primárních aktiv zpracování a předložení:

- a) účelu systému a podmínek jeho provozování,
- b) identifikovaných primárních aktiv a jejich rizik,
- c) ohodnocení přijatelnosti těchto rizik stanovením bezpečnostních parametrů (úrovní) systémem poskytovaných služeb.

(3) Manažer KB je oprávněn vyžadovat od garantů podpůrných aktiv a administrátorů:

- a) identifikování podpůrných aktiv a jejich rizik,
- b) ohodnocení přijatelnosti těchto rizik včetně možnosti přenesení rizik,
- c) vyhodnocení účinnosti kybernetických bezpečnostních opatření.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny

30. 03. 2023	01	Statut Manažera KB	Vytvoření dokumentu
21. 11. 2025	02	Právní oddělení	Úprava dokumentu