Kód:	SR/35/2023	
Číslo jednací:	UTB/23/024491	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Deklarace kybernetické bezpečnosti Univerzity Tomáše Bati ve Zlíně	
Organizační závaznost:	Univerzita Tomáše Bati ve Zlíně	
Datum vydání:	8. 11. 2023	Verze: 01
Účinnost:	13. 11. 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) Deklarace kybernetické bezpečnosti Univerzity Tomáše Bati ve Zlíně (dále jen „Deklarace“) 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 směrnice je deklarovat a schválit základní principy bezpečnosti pro provoz významných informačních systémů (dále jen „VIS“) na UTB. Deklarace je výchozím dokumentem pro bezpečnostní politiky a bezpečnostní dokumentaci realizující KB na UTB.

(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
Závaznost

(1) Povinnost řídit se zákonem o kybernetické bezpečnosti má orgán nebo osoba uvedená v § 3 zákona o kybernetické bezpečnosti. Tento orgán nebo osoba spolupracuje a postupuje alespoň v rozsahu stanoveném v zákoně o kybernetické bezpečnosti. UTB je v souladu s ustanovením § 3 písm. e) zákona o kybernetické bezpečnosti určena jako správce a provozovatel VIS.

(2) UTB jako správce a provozovatel VIS implementuje a provádí bezpečnostní opatření, hlásí kontaktní údaje, hlásí kybernetické bezpečnostní incidenty a provádí opatření v rozsahu stanoveném v zákoně o kybernetické bezpečnosti. Úřadem provádějícím kontrolu je Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“).

(3) Touto směrnicí UTB deklaruje zájem o plošné řešení problematiky KB. Deklarace byla zpracována společně s navazujícími bezpečnostními politikami a bezpečnostní dokumentací.

(4) Tato Deklarace je závazná pro všechny zaměstnance UTB.

Článek 3
Rozsah působnosti

(1) K zajištění a podpoře KB se UTB řídí touto směrnicí, která:
   a) popisuje a vysvětluje zajištění bezpečnosti VIS UTB,
   b) popisuje role a kompetence k zajištění a výkonu agendy KB na UTB,
   c) stanovuje bezpečnostní strategii,
   d) stanovuje cíle a postupy bezpečnostní strategie,
   e) uvádí strukturu bezpečnostních politik a bezpečnostní dokumentace,
   f) zahrnuje způsob revize této směrnice.

(2) Problematika KB pokrývá celou strukturu UTB ve všech lokalitách jejího působení, včetně spolupracujících organizací, které přichází do styku s VIS UTB.

(3) KB se dotýká všech identifikovaných aktiv UTB, a to v míře a rozsahu odpovídajícím významu daného aktiva.

Článek 4
Role a kompetence

(1) K zajištění a výkonu agendy KB na UTB je zřízena role Manažera kybernetické bezpečnosti (dále jen „Manažer KB“) a poradní sbor Výbor pro řízení kybernetické bezpečnosti (dále jen „Výbor KB“).

(2) Manažer KB zajišťuje úkony vyplývající z povinností role manažera kybernetické bezpečnosti dle zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti. Veškeré činnosti Manažera KB jsou popsány ve směrnici rektora *Statut Manažera kybernetické bezpečnosti.*

(3) Výbor KB je zřízen rektorem UTB k zajištění řízení KB na UTB ve smyslu zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti. Veškeré činnosti Výboru KB jsou popsány ve směrnici rektora *Statut Výboru pro řízení kybernetické bezpečnosti.*

Článek 5
Bezpečnostní strategie

(1) Pro bezpečnost VIS UTB se zavádí strategie řízení bezpečnosti. Realizace strategie řízení bezpečnosti vychází z identifikace a hodnocení rizik jednotlivých aktiv využívaných pro provozování VIS.

(2) Realizace strategie řízení bezpečnosti je dle zákona o kybernetické bezpečnosti zajišťována těmito bezpečnostními opatřeními:
   a) organizační opatření,
   b) technická opatření.

(3) Organizačními opatřeními se dle zákona o kybernetické bezpečnosti rozumí:
   a) systém řízení bezpečnosti informací,
   b) řízení rizik,
   c) bezpečnostní politika,
   d) organizační bezpečnost,
   e) stanovení bezpečnostních požadavků pro dodavatele,
   f) řízení aktiv,
   g) bezpečnost lidských zdrojů,
   h) řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,
   i) řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,
   j) akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,
   k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
   l) řízení kontinuity činností,
   m) kontrola a audit kritické informační infrastruktury a významných informačních systémů.

(4) Technickými opatřeními se dle zákona o kybernetické bezpečnosti rozumí:
   a) fyzická bezpečnost,
   b) nástroj pro ochranu integrity komunikačních sítí,
   c) nástroj pro ověřování identity uživatelů,
   d) nástroj pro řízení přístupových oprávnění,
   e) nástroj pro ochranu před škodlivým kódem,
   f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,
   g) nástroj pro detekci kybernetických bezpečnostních událostí,
   h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
   i) aplikační bezpečnost,
   j) kryptografické prostředky,
   k) nástroj pro zajišťování úrovně dostupnosti informací,
   l) bezpečnost průmyslových a řídících systémů.

Článek 6
Cíle a postupy bezpečnostní strategie

(1) Cílem bezpečnostní strategie je zajistit, aby byla KB na UTB řádně vykonávána a nebyl prostřednictvím narušení dostupnosti, důvěrnosti nebo integrity, jakkoliv omezen nebo narušen provoz VIS. Interními opatřeními a postupy pro splnění základních cílů bezpečnostní strategie jsou na UTB prevence, detekce a reakce.

(2) Prevencí se rozumí preventivní opatření snižující identifikovaná rizika v závislosti na možnosti jejich technické a ekonomické realizovatelnosti. Analýza rizik včetně návrhu Plánu zvládaní rizik jsou zpracovávány pravidelně jedenkrát ročně Manažerem KB i v případě podstatných změn v nastavení a konfiguraci VIS UTB. Prioritně jsou využívána technická opatření, organizační opatření jsou zvolena pouze v případě, že ekvivalentní technické opatření neexistuje nebo ho nelze za daných konfiguračních nebo ekonomických podmínek použít.

(3) Detekce spočívá v zavedení organizačních a technických opatření pro zajištění včasného odhalení bezpečnostních událostí a bezpečnostních incidentů VIS UTB. Všechny systémy musí zaznamenávat důležitou činnost uživatelů, funkčnost vlastních SW a HW prostředků. Přijatelné riziko, které není ošetřeno příslušnými preventivními opatřeními, musí být zajištěno kvalitní soustavou opatření pro detekci bezpečnostních událostí a incidentů.

(4) Reakcí se rozumí specifický postup pro šetření, řešení a případně obnovy VIS UTB, primárně s využitím organizačních opatření s určitou mírou využití technických prostředků.

(5) Postupy k zajištění bezpečnostní strategie jsou následující:
   a) zajištění souladu s právními předpisy,
   b) zajištění jednotné ochrany VIS podle požadavků legislativy,
   c) zajištění odpovídajících zdrojů (personálních, technických i finančních) pro oblast KB,
   d) implementaci bezpečnostních technologií a jejich průběžnou aktualizaci a modernizaci,
   e) zajištění schopnosti zvládání bezpečnostních událostí a incidentů,
   f) zajištění adekvátní úrovně důvěrnosti, integrity a dostupnosti,
   g) formalizaci procesů a postupů,
   h) stanovení odpovědností,
   i) zvýšení úrovně bezpečnostního povědomí zaměstnanců.

(6) UTB podporuje stanovené cíle a postupy bezpečnostní strategie a považuje strategii trvalého zajišťování KB jako nedílnou součást vlastních řídících procesů.

Článek 7
Struktura dokumentace

(1) V rámci řízení KB udržuje UTB následující systém dokumentace:
   a) bezpečnostní politiky,
   b) bezpečnostní dokumentace.

(2) Bezpečnostní politiky jsou vydávány formou vnitřních norem rektora v následujícím povinném rozsahu:
   a) Politika systému řízení bezpečnosti informací,
   b) Politika řízení aktiv,
   c) Politika organizační bezpečnosti,
   d) Politika řízení dodavatelů,
   e) Politika bezpečnosti lidských zdrojů,
   f) Politika řízení provozu a komunikací,
   g) Politika řízení přístupu,
   h) Politika bezpečného chování uživatelů,
   i) Politika zálohování a obnovy a dlouhodobého ukládání,
   j) Politika bezpečného předávání a výměny informací,
   k) Politika řízení technických zranitelností,
   l) Politika bezpečného používání mobilních zařízení,
   m) Politika akvizice, vývoje a údržby,
   n) Politika ochrany osobních údajů,
   o) Politika fyzické bezpečnosti,
   p) Politika bezpečnosti komunikační sítě,
   q) Politika ochrany před škodlivým kódem,
   r) Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí,
   s) Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
   t) Politika bezpečného používání kryptografické ochrany,
   u) Politika řízení změn,
   v) Politika zvládání kybernetických bezpečnostních incidentů,
   w) Politika řízení kontinuity činností.

(3) Bezpečnostní dokumentace je vedena v následujícím povinném rozsahu:
   a) Zpráva z auditu kybernetické bezpečnosti,
   b) Zpráva z přezkoumání systému řízení bezpečnosti informací,
   c) Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik,
   d) Zpráva o hodnocení aktiv a rizik,
   e) Prohlášení o aplikovatelnosti,
   f) Plán zvládání rizik,
   g) Plán rozvoje bezpečnostního povědomí,
   h) Evidence změn,
   i) Hlášené kontaktní údaje,
   j) Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků.

Článek 8
Revize

(1) Revize Deklarace se provádí nejméně jednou ročně. Za provedení revize tohoto dokumentu odpovídá Manažer KB, konečnou verzi dokumentu schvaluje Výbor KB. I v případě, že nedojde k žádným změnám, musí být u verze uvedeno datum přezkoumání.

(2) Revize:

a) je zaměřena na bezpečnostní politiky a bezpečnostní dokumentaci,
b) je zaměřena na zajištění souladu technických a organizačních opatření s bezpečnostními politikami a bezpečnostní dokumentací,
c) zahrnuje návrhy možností ke zlepšení KB na UTB,
d) zahrnuje návrhy změn v provozovaném VIS na UTB.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny
30. 10. 2023	01	Manažer KB	Vytvoření dokumentu