Kód:	SR/13/2024	
Číslo jednací:	UTB/24/007646	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika řízení provozu a komunikací	
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:	Právní oddělení, Centrum výpočetní techniky	
Počet stran:	3	
Počet příloh:	1	
Rozdělovník:	zaměstnanci UTB	
Podpis oprávněné osoby:	prof. Mgr. Milan Adámek, Ph.D., v.r.	

Článek 1
Úvodní ustanovení

(1) Politika řízení provozu a komunikací 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“) v podmínkách Univerzity Tomáše Bati ve Zlíně (dále jen „UTB“).

(2) Účelem politiky je zajistit spolehlivý, stabilní a bezpečný provoz významného informačního systému (dále jen „VIS“) a podpůrných aktiv tak, aby byla zaručena bezpečnost primárních aktiv.

(3) Tato politika se vztahuje na 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
Pravomoci a odpovědnosti spojené s bezpečným provozem

(1) Za řízení provozu VIS podle čl. 1 odst. 2 této politiky odpovídá ředitel Centra výpočetní techniky. Tuto odpovědnost je možné dále delegovat určením garantů primárních a podpůrných aktiv.

(2) Za bezpečnost provozu a zejména za řízení kybernetické bezpečnosti odpovídá Manažer kybernetické bezpečnosti (dále jen „Manažer KB“).

Článek 3
Postupy bezpečného provozu

(1) Pro řízení, správu a monitorování aktiv VIS jsou vytvořeny pracovní postupy, které jsou dokumentovány v provozní dokumentaci. Pracovní postupy jsou dostupné všem dotčeným zaměstnancům. Za vedení provozní dokumentace, která je chráněným dokumentem, odpovídá příslušný Garant primárního aktiva.

(2) Pracovní postupy bezpečného provozu zahrnují zejména:

a) práva a povinnosti zaměstnanců, kteří jsou uživateli VIS v konkrétně určených rolích specifikovaných v *Příloze č. 1*, včetně administrátorů,
b) postupy pro spuštění a ukončení chodu VIS, pro restart nebo obnovení chodu VIS po selhání a pro ošetření chybových stavů nebo mimořádných jevů,
c) postupy pro sledování kybernetické bezpečnostní události a kybernetického bezpečnostního incidentu a pro ochranu přístupu k záznamům o těchto činnostech,
d) kontaktní údaje zaměstnanců, kteří jsou určeni jako podpora při řešení neočekávaných systémových nebo technických problémů,
e) postupy řízení a schvalování provozních změn.

(3) Provozní dokumentaci tvoří zejména:

a) *Provozní deník*,
b) *Plán kontrol řízení provozu*,
c) *Evidence kontrol řízení provozu*,
d) *Zálohovací plán*,
e) komunikační matice pro případ vzniku neočekávaných provozních nebo technických problémů,
f) speciální instrukce pro zacházení s výstupy a médii,
g) procedury pro restart a obnovu v případě selhání VIS.

(4) Nákup služeb potřebných pro zajištění provozu VIS probíhá v souladu se zákonem č. 134/2016 Sb. o zadávání veřejných zakázek a vnitřními normami UTB a realizují se výhradně na základě písemných smluv s jasně stanovenými a měřitelnými kritérii dodávek.

Článek 4
Požadavky a standardy bezpečného provozu

(1) Všechny řídicí dokumenty v oblasti bezpečnosti provozu informačních a komunikačních technologií jsou podřízeny jednotné formě řízení dokumentace. Řízení dokumentace jednoznačně určuje správce každého dokumentu. Správci jednotlivých dokumentů mají odpovědnost za určení platnosti dokumentu, struktury dokumentu, zaměstnanců a útvarů, podílejících se na schválení dokumentu a pravidel pro manipulaci s dokumentem.

(2) Řídicí dokumenty v oblasti bezpečnosti provozu informačních a komunikačních technologií jsou v závislosti na oblasti působnosti rozděleny do tří základních úrovní:

a) řízení kapacit,
b) řízení technických zranitelností,
c) řízení změn.

(3) Vývojové a testovací prostředí musí být odděleno od provozního prostředí.

Článek 5
Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů

(1) Audit kybernetické bezpečnosti a bezpečnostní testy musí vždy provádět osoba kvalifikovaná k této činnosti a současně kvalifikovaná k provádění auditu nebo testování technických zařízení. Auditor kybernetické bezpečnosti splňuje minimálně požadavky uvedené v příloze č. 6 vyhlášky o kybernetické bezpečnosti.

(2) Audit kybernetické bezpečnosti a bezpečnostní test nesmí omezit provoz a bezpečnost auditovaného VIS. O provádění auditu musí být informováni s dostatečným předstihem všichni dotčení zaměstnanci zajišťující provozní podporu dotčených systémů a s prováděním auditu musí vyslovit souhlas Manažer KB.

(3) Audit kybernetické bezpečnosti a provozní testy není možné provádět v době, kdy probíhá bezpečnostní incident, případně kdy jsou aplikována neodkladná opatření ke zmírnění dopadů technických zranitelností.

(4) Přístupy Auditora kybernetické bezpečnosti jsou monitorovány a logovány, a současně veškeré požadavky, postupy a odpovědnosti jsou dokumentovány.

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