Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-006**
Název dokumentu:	**Politika řízení provozu a komunikací**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Tato politika se vztahuje na všechny administrátory informačních a komunikačních systémů a osoby zastávající bezpečnostní role.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 10
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	3 + 0
Verze:	1.1
Význam a benefity:	Bezpečné řízení datového provozu a bezpečné řízení počítačové sítě mají zásadní význam pro stabilitu procesů organizace, proto se jedná o klíčovou oblast řízení.
Uložení:	Sekce kyberbezpečnosti na Wiki JU
Ruší dokumenty:	-
Zpracovatel:	Manažer KB JU
Přezkoumal:	Výbor pro kybernetickou bezpečnost JU
Schválil:	Výbor pro kybernetickou bezpečnost JU

Informační vyhlášení

Účelem politiky řízení provozu a komunikací je:

- zajistit bezpečný provoz informačních a komunikačních systémů,
- minimalizovat riziko selhání informačních a komunikačních systémů,
- chránit důvěrnost, integritu a dostupnost informací a
- zabezpečit datové sítě.[1]

a) Pravomoci a odpovědnosti spojené s bezpečným provozem

Za řízení provozu informačního a komunikačního systému odpovídá ředitel Centra informačních technologií („CIT“). Tuto pravomoc je možné dále delegovat. Je nutné stanovit dohledatelný kontakt na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory.

Za bezpečnost provozu a zejména za řízení kybernetické bezpečnosti odpovídá Manažer kybernetické bezpečnosti.

Bezpečnostní operace v sobě zahrnují soubor technických, procesních a dalších opatření, jež jsou základem bezpečného fungování VIS v prostředí VVŠ. Je tedy nutné stanovit pravomoci a odpovědnost za bezpečnostní operace spolu s kontaktními údaji k příslušné podpoře v případě neočekávaných bezpečnostních incidentů.

V rámci bezpečnostních opatření je stanoven kontakt (tzv. “security contact”) pro hlášení bezpečnostních incidentů koncovými uživateli a externími spolupracujícími osobami a společnostmi. Kontakt musí být dobře označený a dohledatelný např. na webových stránkách organizace.

b) Postupy bezpečného provozu

Pro bezpečné řízení provozu VIS jsou vytvořeny pracovní postupy, respektující bezpečnostní zásady a požadavky, stanovené bezpečnostní politikou a vlastníky dat.

Obecně musí postupy bezpečného provozu zahrnovat:

- postupy řízení změn (detailněji popsáno v Politice řízení změn);
- postupy pro zotavení se z incidentů nebo chyb;
- postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů;
- postupy pro sledování kybernetických bezpečnostních událostí a opatření pro ochranu přístupu k záznamům o těchto událostech;
- pravidla a postupy pro ochranu před škodlivým kódem (detailněji popsáno v Politice ochrany před škodlivým kódem);
- postupy pro řízení technických zranitelností;
- postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů;
- pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu;
- postupy pro instalaci technických aktiv;

[1] Zdroj: Vzorová politika provozní bezpečnosti MZČR, příloha č.1.

- postupy pro provádění pravidelného zálohování a kontroly použitelnosti provedených záloh (detailněji popsáno v Politice zálohování a obnovy a dlouhodobého ukládání) a
- pravidla a postupy pro zajištění bezpečnosti síťových služeb (detailněji popsáno v Politice bezpečnosti komunikační sítě).

c) Požadavky a standardy bezpečného provozu

1. řízení změn

Řízení změn je podrobněji zpracováno v Politice řízení změn.

2. řízení zálohování

Zálohování je podrobněji zpracováno v Politice zálohování a obnovy a dlouhodobého ukládání.

3. řízení kapacit

JU musí sledovat své kapacitní požadavky a následně provádět prognózy případných budoucích požadavků, aby mohla zajistit dostatečný výkon, šířku pásma a kapacitu pro ukládání dat. Musí sledovat využití klíčových systémových zdrojů (souborových serverů, doménových serverů, e-mailových serverů apod.), pro to, aby bylo možné uvést do provozu dostatečnou kapacitu v případě potřeby nebo naplánovat kapacitně náročné činnosti na jiné období.

4. oddělení vývojového, testovacího a provozního prostředí

JU musí v rámci své organizační struktury oddělit vývojová a testovací prostředí od provozních (produkčních). Tyto procesy mají za cíl minimalizovat výskyt rizik souvisejících s náhodnými změnami nebo neautorizovaným přístupem k provozním softwarům a citlivým datům.

Musí být definována a zdokumentována pravidla pro přenos softwaru z vývojového do provozního stavu.

Je přísně zakázáno instalovat a provozovat v provozním prostředí programy, které nebyly schváleny k provozu v provozním prostředí. Veškeré zkoušení a testování programů probíhá v testovacím prostředí.

Hesla pro vývojové, testovací a provozní prostředí se musí lišit. Testovací prostředí musí být stabilní a co nejvěrněji napodobovat provozní.

d) Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů

Audit kybernetické bezpečnosti a bezpečnostní testy musí vždy provádět osoba kvalifikovaná k této činnosti. Testování musí být řízeno.

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.

O provádění auditu musí být informováni s dostatečným předstihem všichni dotčení pracovníci zajišťující provozní podporu dotčených systémů.

Historie revizí

Historie revizí je uvedena u souboru této politiky na Wiki JU.