Politika řízení provozu a komunikací

I. Úvodní ustanovení

1) Politika řízení provozu a komunikací stanovuje postupy a protokoly podporující účinnou správu aktiv dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále také *„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 také *„vyhláška o kybernetické bezpečnosti"*) v podmínkách Univerzity Hradec Králové (dále také *„UHK"*).

2) Účelem politiky je:

   a) zajistit spolehlivý, stabilní a bezpečný provoz významných informačních systémů (dále také *„VIS"*) a podpůrných aktiv tak, aby byla zaručena bezpečnost primárních aktiv,

   b) minimalizovat riziko selhání informačních a komunikačních systémů,

   c) chránit důvěrnost, integritu a dostupnost informací a

   d) zabezpečit ochranu komunikační sítě.

3) Tato politika se vztahuje na všechny zaměstnance UHK, informační aktiva vytvořená nebo používaná v rámci VIS, a na uživatele těchto aktiv.

II. Pravomoci a odpovědnosti spojené s bezpečným provozem

1) Aplikační správce VIS v rámci řízení provozu a komunikací pomocí technických nástrojů pro zaznamenávání činností IS, jejich uživatelů a administrátorů pravidelně vyhodnocuje získané informace a na zjištěné nedostatky reaguje v souladu s postupy zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.

2) Aplikační správce VIS v rámci řízení provozu a komunikací zajišťuje bezpečný provoz VIS. Za tímto účelem stanoví pravidla a postupy v provozní dokumentaci a bezpečnostní dokumentaci.

III. Postupy bezpečného provozu

1) Pro řízení, správu a monitorování aktiv VIS jsou vytvořeny pracovní postupy, respektující bezpečnostní zásady, stanovené rektorským výnosem upravujícím *bezpečnostní politiku kybernetické bezpečnosti*[1] a bezpečnostní požadavky, stanovené Garanty primárních a podpůrných aktiv. Pracovní postupy jsou dostupné všem dotčeným zaměstnancům. Za vedení provozní dokumentace odpovídá příslušný aplikační správce VIS.

2) Provozní dokumentaci tvoří zejména:

   a) Provozní deník,

   b) Plán kontrol řízení provozu,

   c) Evidence kontrol řízení provozu,

   d) Plán zálohování,

   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.

3) Postupy bezpečného provozu zahrnují zejména:

   a) práva a povinnosti zaměstnanců, kteří jsou uživateli VIS včetně aplikačních správců VIS a 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.

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

IV. Požadavky a standardy bezpečného provozu

1) Řízení technických zranitelností probíhá na základě seznamů známých technických zranitelností používaných oddělením informačních technologií a využívá následující zásady:

[1] V době vydání této politiky je interním řídicím aktem upravujícím bezpečnostní politiku kybernetické bezpečnosti rektorský výnos č. XXX/2024.

a) aplikační správce VIS průběžně monitoruje informace o technických zranitelnostech ze stanovených zdrojů, identifikuje rizika a navrhuje metody řešení,

b) v závislosti na naléhavosti reakce na zranitelnost je implementováno řešení v rámci postupů pro řízení změn nebo postupů reakce na kybernetický bezpečnostní událost a kybernetický bezpečnostní incident,

c) všechny činnosti jsou automaticky zaznamenány pro pozdější vyhodnocení,

d) efektivnost a účinnost systému správy technických zranitelností je monitorována a posuzována v rámci přezkoumání systému řízení bezpečnosti informací (dále také *„SŘBI*").

2) Řízení kapacit je založeno na stanovení kapacitních nároků pro každý IS. Aplikační správce VIS odpovídá za celkové sledování kapacit, předpokládaný vývoj a návrh případných nápravných opatření.

3) Vývojové a testovací prostředí musí být odděleno od provozního prostředí. V provozním prostředí nesmí být dostupné nástroje pro vývoj, jako jsou například kompilátory. Provozní a projektová dokumentace stanoví, za jakých podmínek dochází k přesunu systému z fáze vývoje a testování do provozního stavu.

V. Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů

1) Audity 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 (dále také *„Auditor KB*") musí splňovat minimálně požadavky uvedené v příloze č. 6 vyhlášky o kybernetické bezpečnosti.

2) Audity kybernetické bezpečnosti a bezpečnostní testy nesmí omezit provoz a bezpečnost auditovaného VIS.

3) O provádění auditu musí být informováni s dostatečným předstihem všichni dotčení zaměstnanci UHK zajišťující provozní podporu dotčených systémů. S prováděním auditu musí vyslovit souhlas Manažer KB.

4) Audity KB a provozní testy není možné provádět v době, kdy probíhá kybernetický bezpečnostní incident, případně kdy jsou aplikována neodkladná opatření ke zmírnění dopadů technických zranitelností.

5) V případě, že Auditor KB potřebuje jiný typ přístupu než pouze pro čtení, vyhotoví provozovatel VIS kopie požadovaných souborů a předá je Auditorovi KB. Kopie souborů se po ukončení auditu smažou nebo, pokud je to vyžadováno Auditorem KB pro dokumentaci auditu, musí být řádným způsobem chráněny.

6) Přístupy Auditora KB jsou monitorovány a logovány. Veškeré požadavky, postupy a odpovědnosti Auditora KB jsou dokumentovány.

VI. Závěrečná ustanovení

Politika řízení provozu a komunikací vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

prof. Ing. Kamil Kuča, Ph.D., v. r.
rektor