

# Statut Manažera kybernetické bezpečnosti

## I. Úvodní ustanovení

- 1) Manažer kybernetické bezpečnosti (dále jen „*Manažer KB*“) Univerzity Hradec Králové (dále jen „*UHK*“) zajišťuje úkony vyplývající z povinností bezpečnostní 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 KB*“) a vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „*vyhláška KB*“).
- 2) Pozice Manažera KB může být vykonávána zaměstnancem UHK, případně zajišťována prostřednictvím externího subjektu – fyzické či právnické osoby.
- 3) Manažer KB je podřízen rektorovi UHK a při plnění své funkce se řídí jeho pokyny v souladu s požadavky právních předpisů a interních předpisů norem v podmínkách UHK.
- 4) Manažer KB je pověřen komunikovat s regulačními orgány v oboru oblasti kybernetické a informační bezpečnosti, zejména s Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „*NÚKIB*“) a s GovCERT/CSIRT, včetně případů řešení kybernetických bezpečnostních událostí a incidentů.

## II. Práva a povinnosti Manažera KB

- 1) Manažer KB odpovídá za plánování, organizování a řízení realizace kybernetických a informačních bezpečnostních projektů a programů schválených Výborem KB na základě pokynů rektora tak, aby bylo dosaženo cílů stanovených zákonem KB a jeho prováděcími předpisy, a to ve stanoveném termínu a v rámci stanoveného rozpočtu. Role Manažera KB působí jako kontaktní osoba pro veškeré aspekty a otázky kybernetické bezpečnosti a prosazuje a koordinuje úlohu systému řízení bezpečnosti informací (dále jen „*SŘBI*“) v podmínkách UHK.
- 2) Manažer KB odpovídá za tvorbu a prosazování SŘBI od průzkumu a analýz, přes průběžné testování prevence až po eliminaci následků a vyhodnocení kybernetických incidentů na UHK.

- 3) Manažer KB odpovídá za tvorbu, prosazování a zajišťování aktualizace vnitřních norem v oblasti kybernetické bezpečnosti UHK v souladu s aktuální právní úpravou v oblasti kybernetické a informační bezpečnosti.
- 4) Manažer KB spolupracuje při identifikaci aktuálního rozsahu a úplnosti informací o aktivech, identifikaci zdrojů, a návrhu na způsoby doplnění chybějících informací (information asset management).
- 5) Manažer KB odpovídá za zajištění schopnosti UHK implementovat bezpečnostní opatření (organizační a technická) ukládaná zákonem KB a za včasnou a hospodárnou implementaci těchto bezpečnostních 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 každý rok Výboru pro řízení kybernetické bezpečnosti (dále také jen „Výbor KB“).
- 7) Manažer KB je oprávněn stanovit:
  - rozsah a hranice SŘBI (s ohledem na aktiva a organizační bezpečnost), ve kterém určí, kterých organizačních částí a technických prvků se SŘBI týká,
  - jednotnou metodiku pro identifikaci a hodnocení aktiv a metodiku pro stanovení kritérií pro přijatelnost rizik,
  - cíle kontinuity činností a strategii (plán) řízení kontinuity další činnosti pro oblast informační a kybernetické bezpečnosti,
  - provozní pravidla a postupy SŘBI,
  - 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 UHK.
- 9) Manažer KB spolupracuje při procesu řízení rizik, jejich rozsahu a dopadu.
- 10) Manažer KB koordinuje proces řešení kybernetické bezpečnostní události nebo kybernetického incidentu a rozhoduje o způsobu řešení.
- 11) Manažer KB rozhoduje o realizaci bezpečnostního opatření na základě informací z monitorovacích a dohledových systémů, rozhodnutí Výboru KB nebo rozhodnutí NÚKIB.

12) Manažer KB zajišťuje:

- detekci kybernetických bezpečnostních událostí a incidentů,
- zpracovávání Zpráv o hodnocení aktiv a rizik, Plán zvládání rizik a Prohlášení o aplikovatelnosti, které obsahuje přehled zavedených bezpečnostních opatření,
- pravidelné hodnocení rizik u dodavatelů, provádění kontrol zavedených bezpečnostních opatření u poskytovaných služeb a odstraňování zjištěných nedostatků,
- aktualizaci SŘBI a příslušné dokumentace dle výsledků auditů nebo významných změn a vyhodnocení vhodnosti a účinnosti bezpečnostních opatření,
- aktualizaci Zprávy o hodnocení aktiv a rizik, Bezpečnostní politiky, Plánu zvládání rizik a Plánu rozvoje bezpečnostního povědomí,
- přípravu podkladů pro realizaci reaktivních opatření vydaných NÚKIB a pro realizaci bezpečnostních opatření (organizační a technická),
- součinnost při provádění kontrolních auditů kybernetické bezpečnosti prováděných NÚKIB a jejich analýze.

13) Manažer KB zpracovává Plán rozvoje bezpečnostního povědomí a s tímto plánem seznamuje Výbor KB.

14) Manažer KB koordinuje opatření ke zvýšení bezpečnostního povědomí v podmínkách UHK včetně školení v oblasti kybernetické a informační bezpečnosti a přípravy a personalizace kurzu kybernetické bezpečnosti v LMS systémech UHK.

15) 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 KB a prováděcích předpisů.

16) Manažer KB provádí pravidelný reporting pro vrcholové vedení UHK o aktuálním stavu SŘBI, bezpečnostních incidentech, zjištěných neshodách a nedostatečné efektivnosti bezpečnostních opatření.

17) Manažer KB pravidelně komunikuje s vrcholovým vedením UHK.

18) Manažer KB je výkonným protějškem NÚKIB pro případy řešení kritických kybernetických bezpečnostních událostí.

### **III. Kompetence Manažera KB**

- 1) Manažer KB je oprávněn vyžadovat od Výboru KB rozhodnutí o:
  - přijatelnosti či nepřijatelnosti identifikovaných kybernetických bezpečnostních rizik včetně stanovení ještě přijatelné míry rizika a stanovení limitu finančních prostředků na eliminaci nepřijatelných rizik,
  - prioritách realizace bezpečnostních opatření a navržených bezpečnostních projektů,
  - určení osob pro výkon rolí garantů aktiv,
  - provedení základní identifikace aktiv.
- 2) Manažer KB je oprávněn od garantů primárních aktiv vyžadovat zpracování a předložení:
  - účelu informačního systému a podmínek jeho provozování,
  - identifikovaných primárních aktiv a jejich rizik,
  - ohodnocení přijatelnosti těchto rizik,
  - stanovení bezpečnostních parametrů (úrovně) systémem poskytovaných služeb (SLA a KPI).
- 3) Manažer KB je oprávněn od garantů podpůrných aktiv a administrátorů vyžadovat:
  - identifikování podpůrných aktiv a jejich rizik,
  - ohodnocení přijatelnosti těchto rizik včetně možnosti přenesení rizik,
  - vyhodnocení účinnosti kybernetických bezpečnostních opatření.

Tento rektorský výnos vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 10. listopadu 2023

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