Politika organizační bezpečnosti

I. Úvodní ustanovení

1) Politika organizační bezpečnosti stanovuje bezpečnostní role a jejich odpovědnosti za prosazení a realizaci bezpečnostních opatření ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, 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) Vzhledem ke skutečnosti, že UHK je správcem a provozovatelem VIS, musí mít dle zákona o kybernetické bezpečnosti ustanovenu roli Manažera kybernetické bezpečnosti (dále také *„Manažer KB"*) a Garanta primárního a podpůrného aktiva. Ostatní bezpečnostní role jsou určeny přiměřeně vzhledem k rozsahu a potřebám systému řízení bezpečnosti informací (dále také *„SŘBI"*).

3) Účelem této politiky je:

   a) stanovit a popsat bezpečnostní role, které jsou součástí organizační struktury kybernetické bezpečnosti na UHK a určit jejich povinnosti a odpovědnosti,

   b) definovat způsoby určení bezpečnostních rolí a

   c) popsat vzájemné vztahy jednotlivých bezpečnostních rolí.

II. Určení bezpečnostních rolí a jejich práv a povinností

1) Povinnost zřízení Výboru kybernetické bezpečnosti (dále také *„Výbor KB"*) a ustanovení Manažera KB, Architekta kybernetické bezpečnosti (dále také *„Architekt KB"*), Garantů primárních a podpůrných aktiv a Auditora kybernetické bezpečnosti (dále také *„Auditor KB"*) se řídí zákonem o kybernetické bezpečnosti a vyhláškou o kybernetické bezpečnosti. Určení členů Výboru KB, Manažera KB, Architekta KB a Auditora KB provádí rektor UHK.

2) Jmenování k zastávání bezpečnostní role a jeho odvolání musí být vždy prokazatelné. Jmenovací listiny jsou ukládány v personální složce příslušného zaměstnance UHK.

3) Garanti primárních aktiv jsou na návrh Výboru KB prostřednictvím jeho předsedy prokazatelně jmenováni a odvoláváni rektorem UHK.

4) Garanty podpůrných aktiv navrhuje Manažer KB ve spolupráci s Garanty primárních aktiv a prokazatelně je jmenuje a odvolává předseda Výboru KB. Pro potřeby snazší správy je možné podpůrná aktiva sdružovat a určit jim pouze jednoho garanta aktiva, respektive skupiny aktiv.

5) Zaměstnanci, kteří zastávají bezpečnostní role, mohou svými právy a povinnostmi prokazatelně pověřit jiného zaměstnance. Vlastní bezpečnostní role a konečná odpovědnost však zůstává na zaměstnanci, který byl do bezpečnostní role jmenován.

Výbor KB, jeho práva a povinnosti

6) Výbor KB zajišťuje činnosti spojené s celkovým řízením a rozvojem VIS a významně se podílí na řízení a koordinaci činností spojených s kybernetickou bezpečností informačních systémů na UHK jako celku.

7) Působnost, pravomoci, odpovědnosti a složení členů Výboru KB jsou stanoveny rektorským výnosem upravujícím postavení *Výboru kybernetické bezpečnosti UHK*[1].

8) Členové Výboru KB se pravidelně scházejí, přičemž průběh a výstupy z jednání jsou uchovávány v listinné nebo elektronické podobě.

Manažer KB, jeho práva a povinnosti

9) Manažer KB je bezpečnostní role odpovědná za plánování, organizování a řízení realizace opatření, projektů a programů k řízení bezpečnosti informací tak, aby bylo dosaženo cílů stanovených zákonem o kybernetické bezpečnosti 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, která rovněž prosazuje a koordinuje úlohu SŘBI na UHK.

10) Manažer KB je oprávněn navrhovat organizační opatření upravující činnosti obecně organizačního, administrativního nebo technického charakteru, včetně bezpečnostních aspektů.

11) Klíčové činnosti, pravomoci a odpovědnosti Manažera KB jsou stanoveny v rektorském výnose upravujícím postavení *Manažera kybernetické bezpečnosti UHK*[2].

12) Pro správný výkon této bezpečnostní role je zapotřebí zajistit potřebné pravomoci, odpovědnost a rozpočet.

Architekt KB, jeho práva a povinnosti

13) Architekt KB je odpovědný za návrh implementace bezpečnostních opatření tak, aby byla zajištěna architektura bezpečnosti VIS na UHK.

14) Architekt KB zajišťuje architekturu bezpečnosti VIS:

   a) prováděním kontrol, hodnocením a testováním funkčnosti zavedených bezpečnostních opatření,

   b) vytvářením testovacích postupů a odpovídajících kritérií pro bezpečnou architekturu VIS.

[1] V době vydání tohoto výnosu je interním řídicím aktem upravujícím postavení výboru kybernetické bezpečnosti rektorský výnos č. 16/2023.
[2] V době vydání tohoto výnosu je interním řídicím aktem upravujícím postavení manažera kybernetické bezpečnosti rektorský výnos č. 17/2023.

c) definováním bezpečnostních požadavků na architektonické úrovni při návrhu, vývoji, testování a implementaci nových informačních a komunikačních systémů a změnu stávajících,

d) navrhováním a optimalizací opatření a procesů řešení kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.

15) Architekt KB analyzuje architekturu SŘBI, jeho jednotlivé komponenty, včetně vzájemných vazeb a zodpovídá za tvorbu a údržbu procesně-organizačního a aplikačního modelu architektury bezpečnosti informací.

16) Role Architekta KB může být určena na základě rozhodnutí Vedení UHK. Na UHK není role Architekta KB v současnosti určena.

Auditor KB, jeho práva a povinnosti

17) Auditor KB je odpovědný za provádění auditu kybernetické bezpečnosti. Auditor KB musí být schopen efektivně provádět audity SŘBI na UHK, zpracovávat požadovanou dokumentaci včetně tvorby výstupních auditních zpráv a vyjádření k naplnění požadavků zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti. Tato role přispívá k efektivnější ochraně SŘBI na UHK.

18) Auditor KB posuzuje soulad implementovaných bezpečnostních opatření na UHK s nejlepší praxí, právními předpisy, interními akty řízení, jinými předpisy a smluvními závazky vztahujícími se k prvku VIS, včetně přezkoumání technické shody a dává doporučení pro zajištění souladu s legislativními požadavky.

19) Auditor KB je oprávněn vyžadovat veškerou dokumentaci, která souvisí s realizací auditu.

20) Auditor KB nesmí být stálým členem Výboru KB, avšak je oprávněn se účastnit zasedání Výboru KB a vyžadovat zápisy ze zasedání.

21) Role Auditora KB je oddělena od výkonu dalších bezpečnostních rolí a není slučitelná s rolemi odpovědnými za provoz VIS.

22) Role Auditora KB může být určena na základě rozhodnutí Vedení UHK. Na UHK není role Auditora KB v současnosti určena.

Garant primárního aktiva, jeho práva a povinnosti

23) Každé primární aktivum musí mít přiděleno svého Garanta.

24) Garant primárního aktiva je odpovědný za zajištění rozvoje, použití a bezpečnosti primárního aktiva (zajištění důvěrnosti, dostupnosti a integrity aktiva).

25) Garant primárního aktiva:

    a) poskytuje podklady Manažerovi KB za účelem provedení analýzy rizik pro dané primární aktivum,

    b) ve spolupráci s Manažerem KB stanoví hodnotu aktiva z pohledu důvěrnosti, integrity a dostupnosti primárního aktiva,

    c) stanovuje obecné bezpečnostní požadavky a koncepty (např. požadované doby obnovy, matici přístupu k primárnímu aktivu či další požadavky na bezpečné užívání, provoz a rozvoj) pro dané primární aktivum na základě klasifikace,

    d) na základě návrhů Manažera KB, Garanta podpůrného aktiva či bezpečnostního správce schvaluje navržená bezpečnostní pravidla a opatření řešící bezpečnostní požadavky pro dané primární aktivum, respektive související podpůrné aktivum typu aplikační služba,

    e) zodpovídá za použití, rozvoj a bezpečnost aktiva,

    f) informuje Manažera KB o všech změnách aktiva, které mají nebo mohou mít vliv na hodnotu aktiva.

Garant podpůrného aktiva, jeho práva a povinnosti

26) Každé podpůrné aktivum musí mít přiděleno svého Garanta.

27) Garant podpůrného aktiva je odpovědný za zajištění rozvoje, použití a bezpečnosti podpůrného aktiva (zajištění důvěrnosti, dostupnosti a integrity aktiva).

28) Garant podpůrného aktiva:

    a) provádí hodnocení důvěrnosti, integrity a dostupnosti podpůrného aktiva, a to na základě primárního aktiva či nadřazených technologických vrstev podpůrných aktiv, které dané aktivum podporuje,

    b) v souladu s bezpečnostními požadavky a bezpečnostní dokumentací zajistí realizaci bezpečnostních opatření,

    c) zajišťuje správu podpůrného aktiva a je odpovědný za jeho užívání v souladu s bezpečnostními požadavky a dokumentací a v souladu s přidělenou rolí,

    d) informuje Manažera KB o všech změnách aktiva, které mají nebo mohou mít vliv na hodnotu aktiva podpůrného aktiva,

    e) informuje Garanty příslušných podpůrných aktiv nadřazených technologických vrstev.

Aplikační správce, jeho práva a povinnosti

29) Aplikační správce je výkonný zaměstnanec, který podle popisu práce zajišťuje minimálně jednu z níže uvedených činností:

    a) instalaci, konfiguraci, správu, údržbu, a evidenci HW a SW, vč. koordinace servisu,

    b) evidenci veškeré mu svěřené výpočetní techniky a komunikačních prostředků,

    c) zálohování systémového programového vybavení a konfigurací a ochranu záložních médií,

    d) správu a evidenci jím zpracované nebo mu svěřené technické a bezpečnostní dokumentace,

    e) kontrolu auditních záznamů ve shodě s bezpečnostní dokumentací,

    f) archivní kopie auditních záznamů (logů).

30) Aplikační správce zodpovídá za řízení, prosazování a kontrolu bezpečnosti informací v rámci svěřeného aktiva.

31) Aplikační správce udržuje aktuální seznam oprávněných uživatelů s jejich přidělenými přístupovými oprávněními.

32) Aplikační správce stanoví pravidla pro mazání dat a likvidaci technických nosičů dat v souladu s vyhláškou o kybernetické bezpečnosti.

33) Aplikační správce zajišťuje kontrolu dodržování zákonných a licenčních podmínek z hlediska využívání programového vybavení.

Administrátor VIS, jeho práva a povinnosti

34) Administrátor VIS zajišťuje správu, provoz, použití a bezpečnost technického aktiva.

35) Administrátor VIS je odpovědný za realizaci bezpečnostních opatření v provozu VIS.

36) Administrátor VIS, který vystupuje současně v roli Garanta příslušného aktiva, vykonává pokyny příslušného vedoucího zaměstnance a Gestora primárního aktiva.

III. Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí

1) RACI matice bezpečnostních rolí kybernetické bezpečnosti (viz Tabulka č. 1) představuje vazby odpovědností rolí na jednotlivé oblasti SŘBI. Tyto vazby jsou reprezentovány písmeny R / A / C / I:

   a) R (Responsible) – má odpovědnost za přímé provádění svěřeného úkolu,

   b) A (Accountable) – má odpovědnost za to, že daný proces je vykonáván v souladu se schválenou podobou procesu,

   c) C (Consulted) – spolupracuje na procesu,

   d) I (Informed) – je informován o průběhu a výsledku jednotlivých fází procesu.

Oblast	ROLE							
	Výbor KB	Manažer KB	Architekt KB	Auditor KB	Garant primárního aktiva	Garant podpůrného aktiva	Aplikační správce	Administrátor VIS
Řízení kybernetické bezpečnosti	A	R	R / C	I	R	R	R	R
Audit kybernetické bezpečnosti	I	C / I	C / I	A / R	C / I	C / I	C/ I	C / I
Návrh bezpečnostních opatření	A	R	R	I	C	C	C	C
Realizace bezpečnostních opatření	I	A	C	I	R	R	A	R
Zajištění rozvoje, použití a bezpečnosti primárního aktiva	I	C	C	–	A	R	C	R
Zajištění rozvoje, použití a bezpečnosti podpůrného aktiva	I	C	C	–	C	A	C	R

Tabulka č. 1 – RACI matice zákonných bezpečnostních rolí

IV. Požadavky na oddělení výkonu bezpečnostních a provozních rolí

1) Povinnosti a vymezení působnosti jednotlivých rolí SŘBI musí být z důvodu střetu zájmů odděleny, aby se omezily příležitosti pro neoprávněné nebo neúmyslné změny nebo zneužití aktiv.
2) Role Manažera KB a Architekta KB nejsou slučitelné s rolemi odpovědnými za provoz informačního a komunikačního systému a s dalšími provozními či řídicími rolemi.
3) Role Auditora KB není slučitelná s bezpečnostními rolemi:
   a) ve Výboru KB,
   b) Manažera KB,
   c) Architekta KB,
   d) Garanta primárního aktiva,
   e) Garanta podpůrného aktiva.
4) Role Auditora KB není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů.
5) Aplikační správce nesmí být Administrátor nebo Garant stejného aktiva, Architekt KB, Manažer KB.

V. Závěrečná ustanovení

Politika organizační bezpečnosti vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

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