Politika systému řízení bezpečnosti informací

I. Úvodní ustanovení

1) Politika systému řízení bezpečnosti informací stanovuje a rozpracovává požadavky na kybernetickou bezpečnost 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, ve znění pozdějších předpisů (dále také *„vyhláška o kybernetické bezpečnosti*") v podmínkách Univerzity Hradec Králové (dále také *„UHK*").
2) Účelem této politiky je definovat strategické cíle Systému řízení bezpečnosti informací (dále také „SŘBI"), rozsah a hranice SŘBI a další pravidla a postupy související s řízením SŘBI.

II. Cíle, principy a potřeby řízení bezpečnosti informací

1) Cílem SŘBI je zajištění bezpečnosti informací (ve všech jejich formách a fázích zpracování) zpracovávaných ve významných informačních systémech (dále také *„VIS*") UHK za účelem plnění své funkce veřejné vysoké školy.
2) Informace nesmí být dostupné nebo nesmí být odhaleny neautorizovaným jednotlivcům, entitám nebo procesům (princip důvěrnosti), musí být zajištěna jejich přesnost a úplnost (princip integrity) a musí být přístupné a použitelné na žádost autorizované entity (princip dostupnosti).
3) Při zavádění SŘBI se berou v úvahu následující základní principy:
   a) povědomí o potřebě řízení bezpečnosti informací,
   b) přidělení odpovědnosti za bezpečnost informací,
   c) začlenění závazku vedení UHK k řízení bezpečnosti informací,
   d) posouzení rizik, které určuje vhodné kontrolní mechanismy k dosažení přijatelné úrovně rizik,
   e) začlenění bezpečnosti jako základního prvku informačních systémů a komunikačních sítí,
   f) aktivní prevence a odhalování incidentů v oblasti bezpečnosti informací,
   g) zajištění komplexního přístupu k řízení bezpečnosti informací,
   h) průběžné přehodnocování bezpečnosti informací a provádění případných úprav.
4) Potřeby řízení bezpečnosti informací vyplývají z hodnocení aktiv a rizik. V rámci tohoto procesu jsou zhodnoceny hrozby, zranitelnosti a úrovně jednotlivých rizik. Následně jsou definována patřičná nápravná opatření.

5) UHK musí prostřednictvím Výboru kybernetické bezpečnosti (dále také *„Výbor KB"*) účinně snižovat rizika a s nimi spojené možné ztráty způsobené narušením důvěrnosti, integrity a dostupnosti informací, selháním zaměstnanců UHK a poškozením majetku.

III. Rozsah a hranice systému řízení bezpečnosti informací

1) Rozsah a hranice SŘBI jsou definovány objektovým perimetrem a logickým perimetrem. SŘBI se nevztahuje na systém řízení ochrany informací dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

2) Do rozsahu SŘBI v podmínkách UHK patří v rámci VIS následující oblasti:

   a) všechny pořizované a zpracovávané informace,

   b) všechny související procesy, lidské a materiální zdroje a příslušná dokumentace,

   c) osobní údaje zaměstnanců UHK, studentů UHK, účastníků programů celoživotního vzdělávání UHK, uchazečů o studium na UHK a absolventů UHK,

   d) prostory UHK,

   e) zařízení a vybavení ve vlastnictví UHK,

   f) informační a komunikační infrastruktura UHK,

   g) uživatelé VIS UHK,

   h) všichni dodavatelé (včetně subdodavatelů), kteří participují na dodávkách primárních a podpůrných aktiv i ve smyslu poskytovaných služeb.

IV. Pravidla a postupy pro řízení dokumentace

1) Řízení dokumentace a záznamů na UHK probíhá s využitím standardních procesů spisové služby, správy dokumentů a organizačními pravidly. Za řízení procesu dokumentace a záznamů kybernetické bezpečnosti odpovídá Manažer kybernetické bezpečnosti (dále také *„Manažer KB*") ve spolupráci s podatelnou UHK.

2) Bezpečnostní dokumentace je tvořena dokumenty definovanými zákonem o kybernetické bezpečnosti a vyhláškou o kybernetické bezpečnosti.

3) Bezpečnostní dokumentace musí být dostupná všem osobám vykonávajícím na UHK činnosti v oblasti kybernetické bezpečnosti.

4) Bezpečnostní dokumentace je vedena ve spisové službě UHK.

5) Při řízení dokumentace jsou vytvářeny, prosazovány a dodržovány postupy pro:

   a) schvalování dokumentů před jejich vydáním a kontrolu jejich správnosti,

   b) aktualizaci dokumentů v případě potřeby včetně potvrzení jejich platnosti,

   c) přezkoumávání dokumentů v pravidelných intervalech včetně potvrzení jejich platnosti,

   d) zabezpečení označení změn a stavu po poslední revizi dokumentů,

   e) zamezení neúmyslného použití neaktuálních dokumentů a jejich řádné označení, pokud vyvstala potřeba dokumenty uchovávat,

   f) zajištění dostupnosti aktuálních verzí dokumentů,

   g) zajištění čitelnosti a snadné identifikace dokumentů,

   h) zajištění řízení včetně distribuce, řádného označení a oddělení dokumentace od jiných subjektů nutné pro činnost UHK,

   i) zajištění principu minimálních oprávnění k dokumentům (*need to know*).

V. Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací

1) V rámci přípravy strategie řízení kybernetické bezpečnosti budou definovány nároky na finanční i lidské zdroje nutné pro dosažení cílů kybernetické bezpečnosti stanovených v rámci SŘBI. Manažer KB přednese tyto požadavky na zdroje v rámci schvalovacího procesu Výboru kybernetické bezpečnosti (dále také *„Výbor KB*"), ten je oprávněn schválit strategii kybernetické bezpečnosti pouze za předpokladu, že budou zajištěny odpovídající finanční a lidské zdroje pro její implementaci.

2) Zdroje na rozvoj technických aspektů kybernetické bezpečnosti spravuje oddělení informačních technologií (dále také *„OIT*") v rámci svého rozpočtu, zdroje na rozvoj lidských zdrojů, zejména na vzdělávání a školení uživatelů i odborných pracovníků budou alokovány v příslušných kapitolách rozpočtu s pevnou alokací na aktivity související s rozvojem kybernetické bezpečnosti.

3) Čerpání zdrojů alokovaných pro rozvoj kybernetické bezpečnosti podléhá schválení Výboru KB na UHK.

VI. Pravidla a postupy pro provádění auditů kybernetické bezpečnosti

1) Nezávislé audity stavu kybernetické bezpečnosti včetně plnění legislativních požadavků v této oblasti se provádí dle § 16 vyhlášky o kybernetické bezpečnosti v pravidelných intervalech alespoň každé 3 roky a při významných změnách.

2) Audit kybernetické bezpečnosti musí být prováděn osobou vyhovující podmínkám stanovených v § 7 odst. 4 vyhlášky o kybernetické bezpečnosti, která nezávisle hodnotí správnost a účinnost zavedených bezpečnostních opatření. Provádění auditu kybernetické bezpečnosti zajišťuje Auditor kybernetické bezpečnosti (dále také „Auditor KB"), kterým může být zaměstnanec UHK, případně externí subjekt – právnická nebo fyzická osoba.

3) Podrobné plánování a vyhodnocování auditu kybernetické bezpečnosti má v kompetenci Manažer KB společně s vedoucím OIT a řídí se *Metodikou provádění auditu kybernetické bezpečnosti*.

4) V rámci auditu kybernetické bezpečnosti se:

   - provádí a dokumentuje audit dodržování bezpečnostní politiky, včetně přezkoumání technické shody,
   - posuzuje soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy a normami, jinými předpisy a smluvními závazky vztahujícími se k VIS UHK a určí případná nápravná opatření pro zajištění souladu.

5) Zpráva z auditu kybernetické bezpečnosti je předkládána Manažerovi KB a vedení UHK.

6) Výsledky auditu kybernetické bezpečnosti se zohlední v *Plánu rozvoje bezpečnostního povědomí* a *Plánu zvládání rizik*.

VII. Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací

1) Přezkoumání SŘBI je prováděno alespoň 1x ročně a při významných změnách s cílem ověřit účelnost, efektivnost a adekvátnost zavedených bezpečnostních opatření provozovaného SŘBI formou interního auditu pod vedením Manažera KB, případně s využitím outsourcingu formou externího subjektu – právnická nebo fyzická osoba.

2) Předmětem přezkoumání SŘBI jsou primárně:

   - bezpečnostní politiky a bezpečnostní dokumentace,
   - soulad technických a organizačních opatření s bezpečnostními politikami.

3) V rámci přezkoumání SŘBI jsou navrhovány možnosti ke zlepšení a návrhy změn v provozovaném VIS na UHK.

4) Z přezkoumání SŘBI vypracuje Manažer KB zprávu, kterou schvaluje Výbor KB, který ji následně předkládá vedení UHK.

VIII. Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací

1) SŘBI je průběžně monitorován prostřednictvím nastavených procesů a prostředků (podle odstavce V a VI). SŘBI je udržován a zlepšován také prostřednictvím systému řízení neshod a incidentů.

2) Veškerá nápravná opatření vychází ze zprávy z přezkoumání SŘBI. Nápravná opatření jsou projednána Výborem KB, k jednotlivým nápravným opatřením jsou stanoveny osoby odpovědné za zavedení nápravných opatření a dodržení termínu zavedení nápravného opatření.

3) Na vzniklé neshody nebo incidenty navrhuje a realizuje nápravné opatření Manažer KB ve spolupráci s vedoucím OIT. V rámci proaktivního přístupu implementuje Manažer KB také preventivní opatření, jejichž úkolem je vylepšit SŘBI.

4) Nápravná opatření jsou pololetně sledována v rámci schůzí Výboru KB.

IX. Klasifikace a přístup k informacím

1) Klasifikace informací je nástrojem pro zajištění přiměřenosti ochrany informačních aktiv UHK. Na základě stanovených pravidel jsou informace rozdělovány a jsou stanovovány požadavky na jejich ochranu. Klasifikace informací poskytuje uživatelům informaci o nutnosti zvláštního zacházení s nimi.

2) Klasifikace informací a jí odpovídající bezpečnostní opatření musí brát ohled na potřeby UHK, na sdílení informací nebo omezování přístupu k nim, a především na výši potencionálních negativních dopadů při narušení jejich bezpečnosti.

3) Informace a výstupy ze systémů, které zpracovávají klasifikované informace, musí být označovány v souladu s jejich hodnotou a citlivostí.

4) Při vzniku informace, resp. při přijetí informace od třetích stran, zaměstnanec, který informaci přijal, rozhoduje, zda informace vyžaduje zvláštní ochranu na základě posouzení kritičnosti informace.

5) Klasifikační schéma přístupu k informacím určuje tyto stupně klasifikace informací:

   a) **Veřejné** – informace, které jsou přístupné všem zaměstnancům UHK, studentům UHK i veřejnosti a jsou schváleny vlastníkem ke zveřejnění. Informace nevyžadují zvláštní úroveň ochrany z pohledu důvěrnosti. Je však nutné dbát na jejich ochranu z pohledu integrity, aby nedošlo ke zveřejnění informací, které neodpovídají skutečnosti. Přístup k veřejným informacím nesmí být omezován.

   b) **Interní** – informace, které jsou určeny pro interní použití všem zaměstnancům UHK, studentům UHK nebo vybrané skupině, avšak nikoli skrze veřejně dostupné kanály. Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, které jsou vázány příslušnými dohodami o mlčenlivosti a tyto informace potřebují ke splnění smluvní závazků. Příjemce musí při předání nastavit důvěrnost komunikace, která zajistí odpovídající ochranu při přenosu a ukládání.

   c) **Chráněné** – informace nejsou veřejně přístupné a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními. Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout.

X. Závěrečná ustanovení

Politika systému řízení bezpečnosti informací vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

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