Politika řízení aktiv

I. Úvodní ustanovení

1) Politika řízení aktiv 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 této politiky je definovat strategické cíle a postupy řízení aktiv se zaměřením na primární a podpůrná aktiva významných informačních systémů (dále také *„VIS"*) v podmínkách UHK.
3) Tato politika se vztahuje na všechny zaměstnance UHK, informační aktiva vytvořená nebo používaná v rámci VIS, a na uživatele těchto aktiv.

II. Identifikace primárních aktiv

1) Manažer kybernetické bezpečnosti (dále také *„Manažer KB"*) ve spolupráci s vedoucími zaměstnanci UHK identifikuje primární aktiva v agendách UHK.
2) Primární aktiva jsou jedinečná, vycházející z klíčových procesů a činností důležitých pro provoz VIS na UHK. Při jejich identifikaci se vychází z dokumentů např.:
   a) Statutu UHK,
   b) Organizačního a vnitřního řádu UHK,
   c) vnitřních předpisů a norem,
   d) legislativních zdrojů,
   e) dokumentů a publikací NÚKIB,
   f) interních aktů řízení organizace atd.
3) Primární aktivum je jedno ze tří typů:
   a) systém,
   b) informace/agenda,
   c) služba.
4) Manažer KB na základě identifikace primárních aktiv navrhne u každého aktiva, zda patří do systému řízení bezpečnosti informací (dále také *„SŘBI"*).
5) Každé jednotlivé primární aktivum musí mít přiřazeno Garanta primárního aktiva, který musí být uveden v *Registru aktiv*, který je chráněným dokumentem. Přístup k *Registru*

aktiv nebo jeho částem je omezen obvykle na členy Výboru kybernetické bezpečnosti (dále také *„Výbor KB"*), garanty primárních a podpůrných aktiv a vedoucí zaměstnance.

6) Jednotlivé Garanty primárních aktiv určuje Manažer KB ve spolupráci s vedoucími zaměstnanci UHK.

7) Manažer KB předloží Výboru KB k projednání návrh na určení Garantů primárních aktiv.

III. Evidence primárních aktiv

1) Primární aktiva musí být evidována ve vhodném systému evidence aktiv a evidence musí obsahovat minimálně tyto údaje:
   a) ID aktiva,
   b) kategorie aktiva,
   c) název aktiva,
   d) garant aktiva,
   e) hodnocení aktiva z hlediska důvěrnosti, integrity a dostupnosti,
   f) hodnota aktiva,
   g) hodnota dopadů.
2) Manažer KB a Garant primárního aktiva jsou odpovědní za vedení centrální evidence primárních aktiv v elektronické podobě.
3) Evidence primárních aktiv je vedena v *Registru aktiv*.

IV. Hodnocení primárních aktiv

1) Hodnocení identifikovaných primárních aktiv je řízeno a dokumentováno v *Hodnocení aktiv*, které je chráněným dokumentem s omezeným přístupem.
2) Hodnocení primárních aktiv provede Garant primárního aktiva ve spolupráci s Manažerem KB.
3) Hodnocení důležitosti primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti je provedeno na stupnicích dle tabulek, které jsou uvedeny v *Metodice pro identifikaci a hodnocení aktiv a pro hodnocení rizik*.

V. Identifikace podpůrných aktiv

1) Manažer KB identifikuje ve spolupráci s Garantem primárního aktiva a vedoucími zaměstnanci UHK podpůrná aktiva v agendách UHK.
2) Podpůrná aktiva zajišťují existenci primárních aktiv a mohou být společná pro více primárních aktiv.
3) Při identifikaci podpůrných aktiv je nutné vycházet z architektury systému a potřeby pro funkčnost primárního aktiva.
4) Podpůrné aktivum je jedno že šesti typů:

a) HW – technické vybavení,

b) SW – programové vybavení,

c) objekty – prostory, budovy,

d) komunikační prostředky – infrastruktura,

e) lidské zdroje,

f) dodavatelé,

g) externí systémy a služby.

5) Každé jednotlivé podpůrné aktivum musí mít přiřazeno Garanta podpůrného aktiva, který musí být uveden v *Registru aktiv*.

6) Role Garanta podpůrného aktiva může být totožná s rolí správce podpůrného aktiva.

7) Jednotlivé Garanty podpůrných aktiv určuje vedoucí Oddělení informačních technologií (dále také „*OIT*") ve spolupráci s Manažerem KB, Garanty primárních aktiv a vedoucími útvarů zaměstnanců, kteří mají za podpůrná aktiva odpovědnost.

8) Manažer KB předloží Výboru KB k projednání návrh na určení Garantů podpůrných aktiv.

VI. Evidence podpůrných aktiv

1) Podpůrná aktiva musí být evidována ve vhodném systému evidence aktiv a evidence musí obsahovat minimálně tyto údaje:
   a) ID aktiva,
   b) kategorie aktiva,
   c) název aktiva,
   d) garant aktiva,
   e) hodnocení aktiva z hlediska důvěrnosti, integrity a dostupnosti,
   f) hodnota aktiva,
   g) hodnota dopadů.
2) Manažer KB a Garant podpůrného aktiva jsou odpovědní za vedení centrální evidence podpůrných aktiv v elektronické podobě.
3) Evidence podpůrných aktiv je vedena v *Registru aktiv*.

VII. Hodnocení podpůrných aktiv

1) Hodnocení identifikovaných podpůrných aktiv je řízeno a dokumentováno v *Hodnocení aktiv*.
2) Hodnocení provede Garant primárního aktiva s Garantem podpůrného aktiva ve spolupráci s Manažerem KB.
3) Hodnocení podpůrných aktiv musí být v souladu s hodnocením primárních aktiv a hodnotí se minimálně z pohledu důvěrnosti, integrity a dostupnosti na stupnicích dle tabulek, které jsou uvedeny v *Metodice pro identifikaci a hodnocení aktiv a pro hodnocení rizik*.

VIII. Určení vazeb mezi primárními a podpůrnými aktivy

1) Vazby určené mezi primárními a podpůrnými aktivy jsou součástí *Registru aktiv*.
2) Pro analýzu a dokumentaci vlastností, závislostí a složení všech aktiv jsou klíčové pohovory Garanta primárního aktiva, Garanta podpůrného aktiva a vedoucích zaměstnanců odborných oddělení ve spolupráci s Manažerem KB.

IX. Pravidla ochrany jednotlivých úrovní aktiv

1) Podle zákona o kybernetické bezpečnosti jsou stanovena:
   a) pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv:
      - určením způsobů rozlišování jednotlivých úrovní aktiv,
      - stanovením pravidel pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv a
      - stanovením přípustných způsobů používání aktiv,
   b) pravidla ochrany odpovídající úrovni aktiv a
   c) způsoby pro spolehlivé smazání nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv.
2) Aktiva jsou označována v souladu s nastavenými pravidly podle jejich klasifikace.
3) Pravidla ochrany jednotlivých úrovní aktiv jsou odvozena od úrovně hodnocení důvěrnosti, integrity a dostupnosti.
4) Na základě hodnocení aktiv jsou určeny možné způsoby zacházení s jednotlivými aktivy, které obsahují informace a stanoveny možné způsoby likvidace dat pro jednotlivé úrovně aktiv. Způsoby zacházení s jednotlivými aktivy musí být zvoleny přiměřeně k jednotlivým úrovním aktiv. Klasifikaci informací musí provést odpovědný garant primárního aktiva, garant podpůrného aktiva nebo autor informace. Úroveň aktiva ovlivní sdílení informací o aktivu.
5) Pravidla ochrany aktiv, včetně způsobů rozlišování jednotlivých úrovní aktiv, pravidel pro manipulaci a evidenci aktiv podle úrovní aktiv a přípustné způsoby používání aktiv jsou uvedeny v *Klasifikaci aktiv* včetně zacházení s aktivy.
6) Definovaná pravidla pro přijatelné použití aktiv se vztahují na všechny uživatele aktiv, dodavatele a třetí strany a musí být zdokumentována.
7) Všichni zaměstnanci UHK a externí pracovníci jsou povinni se seznámit s klasifikací informací a pravidly pro zacházení s chráněnými informacemi a podle toho s informacemi dále pracovat.

X. Způsoby likvidace dat

1) Pravidla pro mazání dat a likvidaci technických nosičů dat jsou definována v souladu s vyhláškou o kybernetické bezpečnosti a musí nabízet přiměřená bezpečnostní opatření s ohledem na hodnotu a důležitosti aktiv.

2) Pravidla pro likvidaci dat jsou stanovena přiměřeně hodnotě a důležitosti aktiv a zohledňují:

   a) hodnotu aktiva (zejména z pohledu důvěrnosti),

   b) technologii (typy a velikost nosičů informace),

   c) zda se nosič informace nachází pod kontrolou organizace či nikoliv,

   d) zda jsou data součástí dedikovaného nebo multitenantního prostředí,

   e) kdo bude likvidaci dat provádět (interní zaměstnanec, nebo dodavatel),

   f) dostupnost vybavení a nástrojů pro likvidaci,

   g) kapacitu likvidovaných nosičů,

   h) zda je k dispozici vyškolený personál,

   i) časovou náročnost likvidace,

   j) cenu likvidace s ohledem na nástroje, školení, validaci, opětovné využití nosiče informace,

   k) možné způsoby likvidace dat (například zničením nosiče, několikanásobným přepsáním nosiče dat, znečitelněním dat jejich šifrováním a podobně),

   l) použitelné způsoby likvidace dat vzhledem ke stavu nosiče informace (například při poškození zařízení nebude možné použít variantu přepisu informace, ale některý ze způsobů fyzické likvidace).

3) Způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií jsou následující:

   a) Odstranění:

      - odstranění dat tak, aby byla pro systém nedostupná (odstranění datového souboru, vyhození výtisku do odpadu),
      - jde o nejméně bezpečný způsob likvidace dat, informace lze obnovit,
      - není použitelné pro nosiče neumožňující opětovný zápis,
      - použitelný způsob pro úroveň důvěrnosti aktiva: nízká.

b) Přepsání:

- přepsání chráněné informace nahodilými hodnotami,
- jde o středně bezpečný způsob likvidace dat, volně dostupné nástroje neumožňují obnovení informace,
- může být nahrazeno nebo kombinováno bezpečnou likvidací kryptografických klíčů k zašifrované informaci,
- není vhodné pro poškozená média, média neumožňující opětovný zápis nebo média s velkou kapacitou,
- použitelný způsob pro úroveň důvěrnosti aktiva: nízká až kritická.

c) Fyzická likvidace nosiče informace:

- zničení nosiče informace, příp. rozebrání zařízení a zničení nosiče informace, skartace výtisků,
- nejbezpečnější metoda likvidace dat, nosič informace nelze znovu použít, původní informace nelze znovu obnovit,
- použitelný způsob pro úroveň důvěrnosti aktiva: střední až kritická.

XI. Závěrečná ustanovení

Politika řízení aktiv vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

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