UNIVERZITA PARDUBICE	
Směrnice č. 4/2026	
Věc:	Politika bezpečnosti informací – zajišťování kybernetické bezpečnosti na Univerzitě Pardubice
Působnost:	Všechny organizační útvary Univerzity Pardubice a její součásti, zaměstnanci a studenti Univerzity Pardubice
Účinnost:	26. března 2026
Číslo jednací:	UPCE/opo/00003291/2026
Vypracoval:	Ing. Jiří Slanina, manažer kybernetické bezpečnosti
Předkládá:	Ing. Olga Klápšťová, ředitelka CITS
Schválila:	doc. Ing. Liběna Černohorská, Ph.D., prorektorka pro vnitřní záležitosti

ČÁST I
ZÁKLADNÍ USTANOVENÍ

Článek 1
Úvodní ustanovení

Účelem této směrnice je deklarovat vůli Univerzity Pardubice (dále jen „UPCE“) prosadit a řídit kybernetickou bezpečnost v rámci UPCE a stanovit základní principy, pravidla, rozsah řízení kybernetické bezpečnosti a hranice pro její zajištění a udržení.

Tato směrnice je závazná pro všechny zaměstnance a studenty UPCE. Tyto osoby jsou povinny dodržovat zásady a pravidla stanovené touto směrnicí a jejími přílohami.

Článek 2
Předmět úpravy

1. Tato směrnice „Politika bezpečnosti informací – zajišťování kybernetické bezpečnosti na UPCE“ (dále jen „Směrnice“) je vydána na základě zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „Zákon“), a jeho prováděcích právních předpisů, zejména vyhlášky č. 408/2025 Sb., o regulovaných službách, vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností a vyhlášky č. 334/2025 Sb., o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na některé úkony.

2. Tato Směrnice je součástí bezpečnostní politiky v oblasti systému řízení bezpečnosti informací v rámci UPCE.

3. Tato Směrnice určuje v rámci UPCE složení výboru pro řízení kybernetické bezpečnosti (dále jen „Výbor pro řízení KB“) a bezpečnostní role, jejich odpovědnosti a jejich práva a povinnosti související se systémem řízení bezpečnosti informací.

Článek 3
Výklad základních pojmů

1. **Administrátorem** se rozumí privilegovaný uživatel nebo jiná osoba zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva,

2. **Akceptovatelným rizikem** se rozumí riziko, které je přijatelné pro UPCE,

3. **Aktivem** se rozumí fyzický nebo digitální prostředek, dokument, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě,

4. **Bezpečností informací** se rozumí zajištění důvěrnosti, integrity a dostupnosti informací a dat,

5. **Bezpečnostní politikou** se rozumí soubor zásad a pravidel, která určují způsob zajištění ochrany aktiv,

6. **Bezpečnostní role osob ve vztahu k aktivům:**
   a) Garantem primárního aktiva se rozumí osoba nebo vedoucí zaměstnanec útvaru, který nese celkovou odpovědnost za dané primární aktivum z hlediska jeho účelu, využívání a souladu s cíli UPCE,
   b) Garantem podpůrného aktiva se rozumí osoba nebo vedoucí zaměstnanec útvaru, který nese celkovou odpovědnost za dané podpůrné aktivum z hlediska jeho účelu, významu a souladu s potřebami aktiv, která podporuje,
   c) Garantem aktiva (dále též jen jako „Garant“) se rozumí společně Garant primárního aktiva a Garant podpůrného aktiva,
   d) Odborným správcem aktiva (dále též jen jako „Odborný správce“) se rozumí odborně způsobilá pověřená osoba nebo vedoucí zaměstnanec útvaru, který zodpovídá za věcnou a obsahovou správnost aktiva, tj. aby aktivum plnilo svou funkci a odpovídalo potřebám uživatelů a procesů UPCE,
   e) Technickým správcem podpůrného aktiva (dále též jen jako „Technický správce“) se rozumí odborně způsobilá pověřená osoba nebo vedoucí zaměstnanec útvaru, který odpovídá za technickou správu, provoz a implementaci bezpečnostních opatření daného podpůrného aktiva,
   f) Uživatelem se rozumí fyzická nebo právnická osoba nebo orgán veřejné moci, který využívá aktiva UPCE,
   g) Privilegovaným uživatelem se rozumí uživatel, osoba či administrátor, jehož činnost na technickém aktivu může mít významný dopad na bezpečnost regulované služby,
   h) Fyzickou osobou uživatele, autora, původce informace, dokumentu, záznamu nebo složky v elektronické nebo listinné podobě (garantem) se rozumí konkrétní identifikovatelná osoba, která danou informaci, dokument, záznam či složku:
      i. vytvořila (autor, původce),
      ii. užívá, upravuje či spravuje (uživatel),
      iii. nebo jinak zprostředkovala či je za její vznik, obsah či uchování odpovědná.

i) Dalšími bezpečnostními rolemi se rozumí Výbor pro řízení KB, Manažer KB, Architekt KB a Auditor KB.

7. **CIA** se rozumí trojice prvků kybernetické bezpečnosti, které definují tři hlavní cíle ochrany informací:
   C = Confidentiality (Důvěrnost) – ochrana před neoprávněným přístupem
   I = Integrity (Integrita) – ochrana před neoprávněnou změnou
   A = Availability (Dostupnost) – zajištění přístupu k informacím, když jsou potřeba,

8. **Daty** se rozumí záznamy jednání, skutečností nebo informací a soubory takových jednání, skutečností nebo informací, včetně provozních údajů a metadat, zejména v podobě textu, čísel, grafů, obrazů, zvuku a videa,

9. **Hodnocením rizik** se rozumí celkový proces určování, analýzy a vyhodnocení rizik,

10. **Hrozbou** se rozumí jakákoliv potenciální okolnost, událost nebo jednání, které mohou být příčinou kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, a která mohou poškodit, narušit nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo další osoby,

11. **Informací** se rozumí zpracovaná, interpretovaná nebo uspořádaná data, která mají význam a kontext v elektronické nebo listinné podobě,

12. **KB** se rozumí kybernetická bezpečnost,

13. **Kybernetickou bezpečnostní událostí** (dále jen „KBU“) se rozumí událost, která může vyústit v kybernetický bezpečnostní incident,

14. **Kybernetickým bezpečnostním incidentem** (dále také jen „KBI“) se rozumí narušení bezpečnosti informací v kybernetickém prostoru,

15. **Kybernetickým prostorem** se rozumí soubor sítí elektronických komunikací a dalších technologií, ve kterém dochází ke zpracování informací a dat v elektronické podobě,

16. **Podpůrným aktivem** se rozumí aktivum zajišťující fungování primárních aktiv nebo jiných podpůrných aktiv, zejména zaměstnanec, dodavatel, technické aktivum, budova a jiný ohraničený prostor, ve kterém se nachází aktivum regulované služby,

17. **Primárním aktivem** se rozumí aktivum v podobě zpracovávané informace nebo poskytované služby,

18. **Regulovanou službou** se rozumí registrovaná služba, o které tak rozhodl Národní úřad pro kybernetickou bezpečnost podle § 6 odst. 2. Zákona,

19. **Rizikem** se rozumí možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu,

20. **Řízením rizik** se rozumí systematický proces zahrnující hodnocení rizik, zavádění bezpečnostních opatření ke zvládání rizik a komunikaci rizik,

21. **Systémem řízení bezpečnosti informací (dále také jen „SŘBI“)** se rozumí část systému řízení UPCE založená na přístupu k rizikům aktiv, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací,

22. **Technickým aktivem** se rozumí technický nebo programový prostředek anebo vybavení,

23. **Vrcholným vedením** se rozumí rektor, prorektoři a kvestor,

24. **Výzkumem a vývojem** se rozumí provádění aplikovaného výzkumu za účelem využití výsledků tohoto výzkumu pro komerční účely. Pod tento výzkum a vývoj spadá:
    a) Citlivá výzkumná činnost, kterou se rozumí činnost zaměřená na aplikovaný výzkum vojenského materiálu uvedeného v seznamu vojenského materiálu podle zákona o zahraničním obchodu s vojenským materiálem,
    b) Aplikovaný výzkum technologie, kterým se rozumí činnost spadající do některé z technologických oblastí podle doporučení Komise o technologických oblastech s kritickým významem pro hospodářskou bezpečnost EU.

25. **Významnou hrozbou** se rozumí hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál závažně ovlivnit aktiva poskytovatele regulované služby nebo uživatele regulované služby natolik, že způsobí značnou újmu,

26. **Významným dodavatelem** se rozumí ten, kdo poskytovateli regulované služby poskytuje plnění, které je významné z hlediska kybernetické bezpečnosti,

27. **Významnou změnou** se rozumí změna, která má nebo může mít vliv na kybernetickou bezpečnost a obsahuje významné riziko,

28. **Zajišťováním kybernetické bezpečnosti** se rozumí zajištění minimální úrovně kybernetické bezpečnosti aktiv povinné osoby založené na zavedení bezpečnostních opatření,

29. **Zranitelností** se rozumí slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito hrozbou,

30. **Zvládáním kybernetického bezpečnostního incidentu** se rozumí úkony vedoucí k prevenci, detekci, analýze, omezení dopadů incidentu, reakci na incident a následné obnově.

Článek 4
UPCE jako poskytovatel regulované služby a režim poskytovatele regulované služby, ohlášení a registrace regulované služby

1. UPCE je na základě kritérií stanovených pro identifikaci regulovaných služeb podle § 4 odst. 1 písm. a) a b) Zákona, resp. podle přílohy vyhlášky č. 408/2025 Sb., o regulovaných službách, poskytovatelem regulovaných služeb, vyjmenovaných v příloze č. 1 této Směrnice.

2. V souvislosti s identifikovanými regulovanými službami uvedenými v příloze č. 1 této Směrnice UPCE naplnila kritéria poskytovatele regulované služby, na nějž se vztahuje režim vyšších povinností.

3. UPCE jako poskytovatel regulovaných služeb deklaruje, že naplnila podmínky pro ohlášení a registraci těchto služeb dle § 6 Zákona a pro účely vydání rozhodnutí o registraci regulovaných služeb ohlásila prostřednictvím portálu Národního úřadu pro kybernetickou a informační bezpečnost ve lhůtě stanovené Zákonem tuto službu Národnímu úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“).

4. Změny režimu poskytovatele regulované služby a zrušení registrace regulované služby se řídí Zákonem.

Článek 5
Povinnosti UPCE jako poskytovatele regulované služby

1. UPCE jako poskytovatel regulované služby nejpozději do 30 dnů od doručení rozhodnutí Úřadu o registraci regulované služby nahlásí Úřadu:
   a) kontaktní údaje (jméno a příjmení oprávněné nebo pověřené osoby, její role či pracovní pozice vůči poskytovateli regulované služby, její telefonní číslo a e-mailová adresa) fyzických osob, které jsou oprávněny za ni jednat ve věcech upravených Zákonem, a případně také
   b) doplňující údaje, kterými jsou informace o její vlastnické struktuře, technické údaje týkající se regulované služby a informace o jejím geografickém rozšíření a přeshraničním poskytování.

2. UPCE jako poskytovatel regulovaných služeb je povinna hlásit změny pouze těch údajů, které nejsou referenčními údaji vedenými v základních registrech, a to nejpozději do 14 dnů ode dne, kdy došlo k jejich změně.

ČÁST II
ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI

Článek 6
Stanovení rozsahu řízení kybernetické bezpečnosti

1. Součástí rozsahu řízení kybernetické bezpečnosti na UPCE (dále jen „stanovený rozsah“) jsou aktiva související s poskytováním regulované služby.

2. Za účelem vymezení stanoveného rozsahu UPCE:
   a) určila všechna svá primární aktiva,
   b) posoudila, zda primární aktiva souvisí s poskytováním regulované služby, a
   c) u primárních aktiv podle písmene b) určila podpůrná aktiva.

3. UPCE eviduje aktiva, která jsou součástí stanoveného rozsahu a primární aktiva, která byla ze stanoveného rozsahu vyjmuta, včetně důvodů jejich vyjmutí.

4. Platí, že primární aktiva, která ještě nebyla posouzena podle odstavce 2 písm. b), a podpůrná aktiva, která ještě nebyla určena podle odstavce 2 písm. c), jsou součástí stanoveného rozsahu.

5. UPCE jako poskytovatel regulovaných služeb stanovený rozsah pravidelně přezkoumává (minimálně 1x za rok) a aktualizuje.

Článek 7
Bezpečnostní opatření

1. Bezpečnostními opatřeními jsou organizační a technická opatření, jejichž účelem, resp. cílem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv ze strany UPCE.

2. UPCE jako poskytovatel regulované služby je povinna v rámci stanoveného rozsahu zavádět a provádět bezpečnostní opatření vyjmenované v odstavci 5 tohoto článku Směrnice, v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby. UPCE začne plnit povinnost zavádět a provádět bezpečnostní opatření pro každou regulovanou službu vždy nejpozději do 1 roku ode dne doručení rozhodnutí o registraci regulované služby.

3. V případě, že UPCE jako poskytovatel regulované služby zavádí nebo provádí bezpečnostní opatření prostřednictvím dodavatele, je povinen vybírat svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření a zahrnovat požadavky vyplývající z bezpečnostního opatření do smluv s dodavatelem.

4. Obsah bezpečnostních opatření a způsob jejich zavádění a provádění stanoví Úřad vyhláškou č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

5. Pro UPCE jako poskytovatele regulované služby v režimu vyšších povinností jsou

a) <u>organizačními opatřeními:</u>

1. systém řízení bezpečnosti informací,
2. požadavky na vrcholné vedení,
3. stanovení bezpečnostních rolí,
4. řízení bezpečnostní politiky a bezpečnostní dokumentace,
5. řízení aktiv,
6. řízení rizik,
7. řízení dodavatelů,
8. bezpečnost lidských zdrojů,
9. řízení změn,
10. akvizice, vývoj a údržba,
11. řízení přístupu,
12. zvládání kybernetických bezpečnostních událostí a incidentů,
13. řízení kontinuity činností a
14. provádění auditu kybernetické bezpečnosti,

b) <u>technickými opatřeními:</u>

1. fyzická bezpečnost,
2. bezpečnost komunikačních sítí,
3. správa a ověřování identit,
4. řízení přístupových práv a oprávnění,
5. detekce kybernetických bezpečnostních událostí,
6. zaznamenávání událostí,
7. vyhodnocování kybernetických bezpečnostních událostí,
8. aplikační bezpečnost,
9. kryptografické algoritmy,
10. zajišťování dostupnosti regulované služby a
11. zabezpečení průmyslových, řídících a obdobných specifických technických aktiv.

6. UPCE se v rámci zajišťování kybernetické bezpečnosti řídí bezpečnostní politikou a bezpečnostní dokumentací, zejména:
   a) má vytvořenou a schválenou relevantní bezpečnostní politiku dle odstavce 5 písm. a) a b) a vede k ní relevantní bezpečnostní dokumentaci,
   b) pravidelně přezkoumává bezpečnostní politiku a bezpečnostní dokumentaci a zajišťuje jejich aktuálnost,
   c) dodržuje a vynucuje dodržování pravidel a postupů stanovených v bezpečnostní politice a bezpečnostní dokumentaci dle § 6 vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

Článek 8
Hlášení a postup hlášení kybernetických bezpečnostních incidentů

1. UPCE jako poskytovatel regulované služby v režimu vyšších povinností, konkrétně manažer kybernetické bezpečnosti (dále jen „Manažer KB“), je povinen hlásit Úřadu KBI, které se projevily ve stanoveném rozsahu, mají původ v kybernetickém prostoru a nelze u nich ve lhůtě 24 hodin po zjištění KBI vyloučit úmyslné zavinění. Manažer KB je povinen nejpozději do 24 hodin po zjištění KBI předložit prvotní hlášení, v němž uvede své identifikační údaje, základní údaje o KBI a zda se domnívá, že byl KBI způsoben nezákonným zásahem nebo že by mohl mít přeshraniční dopad.

2. Manažer KB poskytne na výzvu Úřadu nezbytné informace a součinnost při zvládání KBI, pokud nelze sledovaného účelu dosáhnout jinak nebo by bylo jinak jeho dosažení podstatně ztížené. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti.

3. Manažer KB eviduje údaje o KBI, KBU, hrozbách a zranitelnostech.

4. V případě, že se jedná o KBI s významným dopadem na kybernetický prostor státu Manažer KB dále předloží:
   a) bez zbytečného odkladu, nejpozději do 72 hodin po zjištění KBI oznámení, v němž aktualizuje informace uvedené v odstavci 1, předloží prvotní posouzení KBI a uvede dopad a indikátory kompromitace, pokud jsou k dispozici,
   b) na výzvu Úřadu nebo Národního CERT průběžnou zprávu o podstatných změnách stavu zvládání KBI a
   c) nejpozději do 30 dnů ode dne předložení oznámení podle písmene a) závěrečnou zprávu o vyřešení KBI; v případě, že po uplynutí uvedené lhůty KBI stále trvá, předloží Manažer KB bez zbytečného odkladu po uplynutí lhůty průběžnou zprávu o aktuálním stavu zvládání KBI, a poté nejpozději do 30 dnů ode dne, kdy došlo k vyřešení KBI závěrečnou zprávu o vyřešení KBI.

5. Manažer KB hlásí KBI, včetně dobrovolných hlášení, prostřednictvím Portálu Úřadu. Pokud nelze využít Portálu Úřadu, zašle Manažer KB hlášení na adresu elektronické pošty Úřadu určenou pro příjem hlášení KBI nebo do datové schránky Úřadu.

Článek 9
Zvládání KBI UPCE, informační povinnost

1. Úřad poskytne bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení Manažera KB, své vyjádření ke KBI.

2. Na žádost Manažera KB poskytne Úřad metodickou podporu k provádění zmírňujících opatření, a případnou další technickou podporu ke zvládání hlášeného KBI.

3. Manažer KB je povinen poskytnout na výzvu Úřadu nezbytné informace a součinnost při zvládání KBI, pokud nelze sledovaného účelu dosáhnout jinak nebo by bylo jinak jeho dosažení podstatně ztížené. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti.

4. Pokud Manažer KB považuje z důvodu zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv za vhodné, oznámí bez zbytečného odkladu uživatelům regulované služby KBI s významným dopadem, který by mohl negativně ovlivnit poskytování této služby. Úřad může UPCE uložit povinnost nebo zákaz informovat uživatele regulované služby o tomto incidentu.

Článek 10
Protiopatření

1. Protiopatření jsou úkony Úřadu, jichž je potřeba k ochraně aktiv před hrozbou nebo před zneužitím zranitelnosti v oblasti kybernetické bezpečnosti nebo před KBI, anebo k řešení již nastalého KBI.

2. Protiopatřeními jsou:
   a) výstraha,
   b) varování a
   c) reaktivní protiopatření.

3. Definice jednotlivých protiopatření jsou obsaženy v příslušných ustanoveních Zákona.

Článek 11
Závěrečná ustanovení

1. Zrušuje se Směrnice č. 7/2021 Základní politika bezpečnosti informací – způsob zajištění kybernetické bezpečnosti na Univerzitě Pardubice.

2. Tato Směrnice nabývá platnosti a účinnosti dnem podpisu rektora.

V Pardubicích dne 26. března 2026

prof. Ing. Libor Čapek, Ph.D.
rektor

Přílohy:

1. Výčet poskytovaných regulovaných služeb UPCE, režim
2. Výčet primárních aktiv UPCE
3. Politika systému řízení bezpečnosti informací (ve zkratce „SŘBI“)
4. Politika požadavků na vrcholné vedení, Statut Výboru pro řízení KB, Jednací řád Výboru pro řízení KB
5. Politika bezpečnostních rolí
    - Statut Manažera kybernetické bezpečnosti
    - Statut Architekta kybernetické bezpečnosti
    - Statut Auditora kybernetické bezpečnosti
    - Určení osob odpovědných za aktiva
    - Statut Garanta
    - Statut Odborného správce
    - Statut Technického správce
6. Politika řízení bezpečnostní politiky a bezpečnostní dokumentace

Výčet poskytovaných regulovaných služeb UPCE, režim

1. UPCE je na základě kritérií stanovených pro identifikaci regulovaných služeb podle § 4 odst. 1 písm. a) a b) Zákona, resp. podle přílohy vyhlášky č. 408/2025 Sb., o regulovaných službách, **poskytovatelem následujících regulovaných služeb:**

   - **v režimu vyšších povinností:**
   a) č. 19., bod 19.1. písm. a) Věda, výzkum a vzdělávání – Výzkum a vývoj,
   b) č. 21., bod 21.1. Obranný průmysl – Výroba vojenského materiálu uvedeného v seznamu vojenského materiálu podle zákona o zahraničním obchodu s vojenským materiálem,
   c) č. 21., bod 21.2. Obranný průmysl – Obchod s vojenským materiálem podle zákona o zahraničním obchodu s vojenským materiálem.

2. UPCE dále poskytuje následující regulovanou službu:
   a) č. 1.1 Výkon svěřených pravomocí,
   která odpovídá režimu nižších povinností; UPCE však naplnila kritéria poskytovatele regulované služby odpovídající režimu vyšších povinností.

Výčet primárních aktiv UPCE

1. Podle výčtu regulovaných služeb, které byly na UPCE identifikovány podle Zákona a příslušných právních předpisů, jsou stanovena primární aktiva UPCE.

2. Primární aktiva představují reálně vykonávané činnosti a procesy, které na UPCE běžně probíhají v rámci výkonu jejích svěřených pravomocí, poskytování vzdělávání, zajišťování vědecké, výzkumné, vývojové, inovační a další související činnosti, jakož i v rámci vnitřního řízení a správy univerzity. Jsou v souladu s posláním, strategickými cíli a zákonnými povinnostmi UPCE.

3. Z pohledu Zákona mají primární aktiva s ohledem na kybernetickou bezpečnost dvojí charakter:
   - charakter služby – představuje poskytování činnosti, funkce nebo výkonu pravomoci vůči interním nebo externím subjektům,
   - charakter informace – je neoddělitelně spojena se zpracováním, uchováváním nebo předáváním informací a dat v elektronické podobě.

4. S těmito primárními aktivy je proto nakládáno ve dvou aspektech:
   - jako se službou UPCE, u níž je potřeba zabezpečit její dostupnost a kontinuitu,
   - jako s informací UPCE, u níž je potřeba zabezpečit její dostupnost, integritu a důvěrnost.

   Jejich ochrana a řízení probíhá prostřednictvím podpůrných aktiv, organizačních opatření a bezpečnostních mechanismů v souladu s touto směrnicí.

5. Ke každému z uvedených primárních aktiv je určen garant primárního aktiva z řad vedení UPCE.

Č.	Primární aktivum	Garant primárního aktiva
1	Výkon svěřených pravomocí	Prorektor pro vzdělávání a kvalitu
2	Vzdělávací činnost	Prorektor pro vzdělávání a kvalitu
3	Vědeckovýzkumná a tvůrčí činnost	Prorektor pro vědu a tvůrčí činnost
4	Výzkum a vývoj v oblasti obranného průmyslu	Prorektor pro vědu a tvůrčí činnost
5	Výroba vojenského materiálu	Rektor
6	Obchod s vojenským materiálem	Rektor
7	Vnitřní a strategické řízení	Prorektor pro vnitřní záležitosti
8	Vnitřní správa	Kvestor
9	Vnější vztahy	Prorektor pro vnější vztahy

Politika systému řízení bezpečnosti informací (ve zkratce „SŘBI“)

1. Definice rozsahu SŘBI podléhá schválení Výboru pro řízení KB a musí obsahovat veškerá primární aktiva zajišťující poskytované regulované služby provozované na UPCE.

2. Zavedení SŘBI patří mezi stěžejní organizační bezpečnostní opatření pro zajištění řádného poskytování regulovaných služeb a kybernetické bezpečnosti aktiv.

3. V rámci systému řízení bezpečnosti informací UPCE stanovila cíle SŘBI:
   a) zajistit a provádět přiměřená bezpečnostní opatření směřující k zajištění kybernetické bezpečnosti regulovaných služeb a minimalizovat dopady kybernetických bezpečnostních incidentů na jejich poskytování,
   b) zajistit schopnost obnovy regulovaných služeb po kybernetickém bezpečnostním incidentu nebo jiné mimořádné události,
   c) zajistit ochranu informací zpracovávaných při poskytování regulovaných služeb před neoprávněným přístupem a změnou,
   d) zajistit, aby přístup k informačním systémům a informacím byl řízen podle pracovních pozic a principu nezbytné potřeby,
   e) systematicky identifikovat, hodnotit a řídit kybernetická rizika ohrožující regulované služby a jejich podpůrná aktiva v souladu s vyhláškou č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností,
   f) stanovit a schválit bezpečnostní politiky, bezpečnostní dokumentace ve vztahu k řízení kybernetické bezpečnosti a proces řízení výjimek,
   g) zavést efektivní proces detekce, hlášení, analýzy a řešení kybernetických bezpečnostních incidentů,
   h) zvyšovat úroveň povědomí zaměstnanců a studentů o kybernetické bezpečnosti a jejich odpovědnosti při práci s informacemi,
   i) zajistit pravidelné vyhodnocení účinnosti SŘBI formou zprávy z přezkoumání SŘBI, která je předkládána Výboru pro řízení KB a vedení UPCE,
   j) zajistit provedení auditu kybernetické bezpečnosti,
   k) aktualizovat SŘBI na základě zjištění auditů, hodnocení rizik, dopadů incidentů a změn relevantní legislativy.

4. Při zavádění SŘBI UPCE zajistí základní povinnosti uvedené v § 3 vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

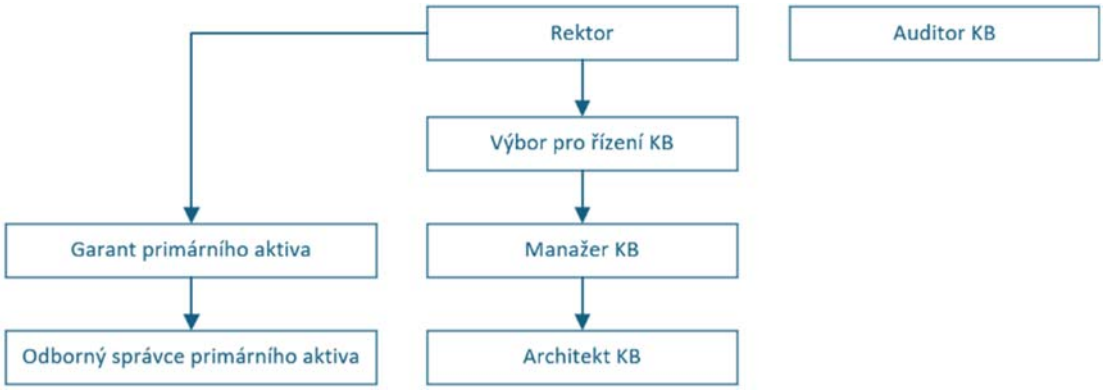
Politika požadavků na vrcholné vedení, Statut Výboru pro řízení KB, Jednací řád Výboru pro řízení KB

Část I – Hierarchie bezpečnostních rolí ve vztahu k aktivům UPCE
Část II – Politika požadavků na vrcholné vedení
Část III – Statut Výboru pro řízení KB
Část IV – Jednací řád Výboru pro řízení KB

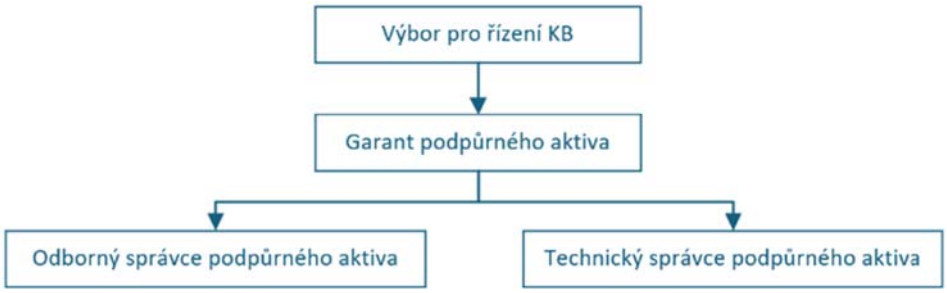
Část I
Hierarchie bezpečnostních rolí ve vztahu k aktivům UPCE

1. Hierarchie je navržena tak, aby umožnila koordinaci aktivit SŘBI v rámci UPCE prostřednictvím osob zastupujících bezpečnostní role.

Obrázek č.1: Hierarchie bezpečnostních rolí ve vztahu k primárním aktivům



Obrázek č. 2: Hierarchie bezpečnostních rolí ve vztahu k podpůrným aktivům



Část II
Politika požadavků na vrcholné vedení

1. Vedení UPCE si uvědomuje důležitost zajištění kybernetické bezpečnosti a zavazuje se k vytvoření podmínek, které umožní naplnění níže uvedených cílů.

2. K uvedeným cílům vedení UPCE patří:
   a) proškolení vrcholného vedení o jeho povinnostech, o bezpečnostní politice, zejména v oblasti SŘBI, řízení rizik a řízení kontinuity činnosti formou vstupních

a pravidelných školení k získání znalostí a dovedností vedoucích k určování rizik a posouzení vhodnosti zvolených postupů při řízení rizik a jejich dopadů na regulovanou službu,

b) zajištění stanovení bezpečnostní politiky a cílů SŘBI, slučitelných se strategickým směřováním UPCE,
c) zajištění začlenění SŘBI do procesů UPCE,
d) zajištění dostatečných finančních zdrojů potřebných pro SŘBI,
e) informování zaměstnanců o významu SŘBI a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,
f) zajištění podpory k dosažení cílů SŘBI,
g) podpora a vedení zaměstnanců k rozvíjení efektivity SŘBI,
h) podílení se na vypracování analýzy dopadů řízení kontinuity činností,
i) zajištění testování plánů kontinuity činností, plánů obnovy a procesů spojených se zvládáním KBI,
j) prosazování neustálého zlepšování SŘBI,
k) podpora osob zastávajících bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti,
l) zajištění stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role,
m) zajištění, aby byla zachována mlčenlivost u všech uživatelů (zejména administrátorů, osob zastávajících bezpečnostní role a dodavatelů),
n) zajištění pravomoci pro osoby zastávající bezpečnostní role potřebné pro naplňování jejich rolí a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů.

3. Vedení UPCE se prokazatelně seznamuje:
   a) se zprávou o přezkoumání SŘBI,
   b) se zprávou o hodnocení rizik,
   c) s výsledky analýzy dopadů a
   d) s výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti.

Část III
Statut Výboru pro řízení KB

Článek 1
Úvodní ustanovení

1. Výbor pro řízení KB je zřízen rozhodnutím rektora k zajištění celkového řízení a rozvoje systému řízení bezpečnosti informací ve smyslu Zákona a jeho prováděcích právních předpisů.

2. Statut Výboru pro řízení KB stanovuje základní okruh jeho působnosti, členství ve Výboru pro řízení KB, organizační zajištění jeho jednání, způsob usnášení a výstupy z jeho jednání.

Článek 2
Složení Výboru pro řízení KB

1. Výbor pro řízení KB má 5 členů, které určí a schvaluje rektor.

2. Členy Výboru pro řízení KB jsou:
   a) Prorektor pro vnitřní záležitosti – předseda Výboru pro řízení KB,
   b) Kvestor – místopředseda Výboru pro řízení KB,
   c) Manažer KB,
   d) Ředitel centra informačních technologií a služeb,
   e) Akademický pracovník UPCE, odborně způsobilý pro celkové řízení a rozvoj systému zajišťování minimální kybernetické bezpečnosti, schválený rektorem na návrh Akademického senátu UPCE, a to na dobu funkčního období rektora.

3. Stálým hostem zasedání Výboru pro řízení KB bez práva hlasovat je rektor, pověřenec pro ochranu osobních údajů a tajemník Výboru pro řízení KB, jehož činnost je upravena v čl. 5 této Přílohy.

4. Členství předsedy a/nebo místopředsedy ve Výboru pro řízení KB zaniká dnem skončení funkčního období rektora, odvoláním nebo vzdáním se funkce.

5. Členství ostatních členů Výboru pro řízení KB zaniká dnem jejich odvolání na návrh rektora po předchozím projednání ve Výboru pro řízení KB, případně jejich odstoupením.

Článek 3
Činnost Výboru pro řízení KB

1. Výbor pro řízení KB zejména:
   a) odpovídá za celkové řízení a rozvoj kybernetické bezpečnosti v rámci UPCE,
   b) odpovídá za tvorbu rámce kybernetické bezpečnosti, směřování a zásad kybernetické bezpečnosti UPCE (definování strategických cílů a směřování rozvoje v oblasti kybernetické bezpečnosti),

c) definuje práva, povinnosti a odpovědnost jednotlivých bezpečnostních rolí v rámci SŘBI,
d) definuje požadavky na podávání zpráv a kontrolu SŘBI,
e) kontroluje aktuální stav kybernetické bezpečnosti v rámci UPCE a zjišťuje, zda dochází k naplňování plánovaných cílů,
f) projednává zprávy z auditu vydané a schválené auditorem KB a zprávy z testování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti.

2. Výbor pro řízení KB dále projednává a předkládá rektorovi:
   a) posouzení přijatelnosti či nepřijatelnosti identifikovaných kybernetických bezpečnostních rizik včetně stanovení přijatelné míry rizika,
   b) návrhy na přidělení finančních prostředků pro oblast kybernetické bezpečnosti navržených Výboru pro řízení KB Manažerem KB,
   c) návrhy na stanovení pořadí důležitosti realizace jednotlivých bezpečnostních opatření a bezpečnostních projektů navržených Manažerem KB.

3. Výbor pro řízení KB projednává a předkládá rektorovi závaznou bezpečnostní dokumentaci v oblasti kybernetické bezpečnosti, a to zejména:
   a) bezpečnostní politiky SŘBI,
   b) seznam informačních a komunikačních systémů zahrnutých do SŘBI,
   c) zprávy z přezkoumání systému zajišťování kybernetické bezpečnosti (nejméně 1 x ročně),
   d) Analýzu rizik a Plán zvládání rizik (nejméně 1 x ročně),
   e) zápis z jednání Výboru pro řízení KB nebo v případě identifikace KBI zprávu o stavu kybernetické bezpečnosti UPCE.

4. V oblasti ochrany osobních údajů[1] má Výbor pro řízení KB následující pravomoci a odpovědnosti:
   a) Výbor pro řízení KB spolupracuje s pověřencem pro ochranu osobních údajů, který je stálým hostem Výboru pro řízení KB a bere na zřetel jeho stanoviska,
   b) vyjadřuje se k návrhům a implementaci bezpečnostních procesů pro ochranu osobních údajů v rozsahu opatření kybernetické bezpečnosti,
   c) informuje vrcholné vedení UPCE o opatřeních v oblasti ochrany osobních údajů v rozsahu opatření kybernetické bezpečnosti,
   d) ve spolupráci s příslušným pověřencem pro ochranu osobních údajů se vyjadřuje k přijatelnosti či nepřijatelnosti identifikovaných rizik ochrany osobních údajů včetně stanovení přijatelné míry rizika, přičemž bere na zřetel stanovisko pověřence pro ochranu osobních údajů,
   e) podává návrh na přidělení finančních prostředků v oblasti ochrany osobních údajů v rozsahu opatření kybernetické bezpečnosti,

[1] Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů; zákon o ochraně osobních údajů.

Článek 4
Práva a povinnosti členů Výboru pro řízení KB

1. Členové Výboru pro řízení KB mají právo podílet se aktivně na činnosti Výboru pro řízení KB, vznášet dotazy, náměty, připomínky k projednávaným zprávám a návrhům, uplatňovat svá stanoviska k řešení problémů týkajících se kybernetické bezpečnosti.

2. Členové Výboru pro řízení KB jsou povinni účastnit se jeho zasedání a plnit úkoly, kterými je Výbor pro řízení KB pověřil.

3. Předseda Výboru pro řízení KB zejména:
   a) řídí a organizuje činnost Výboru pro řízení KB,
   b) vydává stanoviska, doporučení a další dokumenty Výboru pro řízení KB,
   c) úkoluje na základě rozhodnutí Výboru pro řízení KB osoby odpovědné v oblasti kybernetické bezpečnosti a koordinuje jejich plnění s cílem dosažení souladu informačních a komunikačních systémů UPCE s požadavky právních předpisů, vnitřních předpisů a norem UPCE.

4. Na základě jednání Výboru pro řízení KB předkládá předseda Výboru pro řízení KB vrcholnému vedení UPCE schválené návrhy dokumentů či požadavků na uskutečnění výdajů z finančních zdrojů UPCE na zabezpečení nutné míry kybernetické bezpečnosti.

5. V nepřítomnosti předsedy Výboru pro řízení KB plní jeho úkoly místopředseda Výboru pro řízení KB.

Článek 5
Administrace Výboru pro řízení KB

1. Administraci činností Výboru pro řízení KB zajišťuje tajemník Výboru pro řízení KB.

2. Tajemníkem Výboru pro řízení KB je zaměstnanec UPCE, pověřený předsedou Výboru pro řízení KB.

3. Tajemník Výboru pro řízení KB:
   a) zabezpečuje organizační, technické a administrativní záležitosti činnosti Výboru pro řízení KB,
   b) připravuje návrh programu jednání Výboru pro řízení KB,
   c) odpovídá za přípravu a včasné předkládání podkladových materiálů k projednání členům Výboru pro řízení KB podle pokynů předsedy Výboru pro řízení KB,
   d) zpracovává pravidelné informace o činnosti Výboru pro řízení KB,
   e) uchovává výstupy (zápisy, rozhodnutí) ze zasedání v listinné nebo elektronické podobě.

Článek 6
Zasedání Výboru pro řízení KB

1. Zasedání Výboru pro řízení KB jsou svolávána podle potřeby, včetně mimořádného zasedání, na pokyn předsedy Výboru pro řízení KB tajemníkem Výboru pro řízení KB, nejméně však jednou za 3 měsíce.

2. Předseda Výboru pro řízení KB organizuje práci Výboru pro řízení KB a dbá na plnění Výborem pro řízení KB přijatých usnesení. V případě nepřítomnosti předsedy či nutnosti projednání nebo řešení neodkladných záležitostí svolá zasedání místopředseda Výboru pro řízení KB.

3. Program zasedání Výboru pro řízení KB navrhuje předseda Výboru pro řízení KB. Vychází přitom z materiálů předložených k projednání, z návrhů členů Výboru pro řízení KB a úkolů uložených na jeho zasedáních.

4. Odborné podklady pro jednání Výboru pro řízení KB připravují zejména členové Výboru pro řízení KB.

5. Shromažďování a distribuci podkladů pro jednání Výboru pro řízení KB organizuje tajemník Výboru pro řízení KB.

6. Zasedání Výboru pro řízení KB se řídí Jednacím řádem Výboru pro řízení KB.

Část IV
Jednací řád Výboru pro řízení KB

Článek 1
Úvodní ustanovení

Jednací řád Výboru pro řízení KB (dále jen „Jednací řád“) upravuje jeho jednání.

Článek 2
Svolání zasedání Výboru pro řízení KB

1. Zasedání Výboru pro řízení KB svolává na základě pokynu předsedy Výboru pro řízení KB tajemník Výboru pro řízení KB nejméně jedenkrát za 3 měsíce. Návrh na svolání zasedání Výboru pro řízení KB může předsedovi prostřednictvím tajemníka Výboru pro řízení KB podat písemnou formou kterýkoli člen Výboru pro řízení KB, předseda je pak povinen nejpozději do pěti pracovních dnů rozhodnout o svolání Výboru pro řízení KB v nejbližším vhodném termínu. V případě mimořádné bezpečnostní situace může předseda Výboru pro řízení KB svolat mimořádné zasedání Výboru pro řízení KB okamžitě.

2. Na zasedání Výboru pro řízení KB jsou jeho členové, stálí hosté, případně též přizvané osoby, zváni pozvánkou zpravidla 5 pracovních dní předem.

3. Zasedání Výboru pro řízení KB mohou být realizována:
    a) v prezenční formě,
    b) v distanční formě pomocí vhodného prostředku komunikace na dálku, který umožňuje zabezpečený přenos zvuku a obrazu a synchronní komunikaci.

4. O formě zasedání Výboru pro řízení KB rozhoduje předseda Výboru pro řízení KB.

Článek 3
Průběh zasedání a rozhodování Výboru pro řízení KB

1. Zasedání Výboru pro řízení KB řídí zpravidla předseda Výboru pro řízení KB, který může řízením pověřit místopředsedu Výboru pro řízení KB nebo člena Výboru pro řízení KB. Výbor pro řízení KB rozhoduje usnesením. Usnesení musí být doslovně uvedena v zápisu ze zasedání.

2. Výbor pro řízení KB jedná zpravidla na základě předem připravených písemných materiálů, které předkládají členové Výboru pro řízení KB.

3. Výbor pro řízení KB projednává materiály v pořadí podle programu schváleného na začátku zasedání Výboru pro řízení KB.

4. Projednávání každého materiálu zpravidla zahrnuje úvodní slovo předkladatele, dotazy a návrhy účastníků zasedání Výboru pro řízení KB a přijetí usnesení k projednávanému materiálu.

5. Výbor pro řízení KB je způsobilý jednat a přijímat závěry, je-li přítomna nadpoloviční většina všech členů Výboru pro řízení KB.

6. Závěry ze zasedání Výboru pro řízení KB přijímají jeho členové hlasováním, formou usnesení. K přijetí usnesení je třeba nadpoloviční většiny hlasů všech členů Výboru pro řízení KB.

7. Ze zasedání Výboru pro řízení KB pořizuje tajemník Výboru pro řízení KB písemná usnesení a zápis, které zasílá všem účastníkům zasedání Výboru pro řízení KB.

8. Zasedání Výboru pro řízení KB jsou neveřejná.

9. Předseda Výboru pro řízení KB předkládá vrcholnému vedení zprávy, které je Výbor pro řízení KB povinen předložit vedení UPCE z hlediska SŘBI nebo jejichž předložení je zaznamenáno v usnesení.

Článek 4
Schvalování „per rollam“

1. Ve výjimečných případech v mezidobí mezi zasedáními Výboru pro řízení KB, kdy materiály nelze předložit standardním způsobem, může na základě písemné žádosti předkladatele materiálu, podané prostřednictvím tajemníka Výboru pro řízení KB, předseda Výboru pro řízení KB rozhodnout o schválení materiálu „per rollam“ s využitím elektronické formy komunikace.

2. Materiály ke schválení „per rollam“ rozesílá tajemník Výboru pro řízení KB všem členům Výboru pro řízení KB s informací, kdo materiál předkládá, a s pevně stanovenou lhůtou k zaslání stanoviska (souhlasného/nesouhlasného), která činí tři pracovní dny, není-li stanoveno jinak. Své stanovisko zasílají členové Výboru pro řízení KB přímo tajemníkovi Výboru pro řízení KB. Neodpoví-li člen ve stanovené lhůtě, je toto považováno za vyslovení nesouhlasu. Po obdržení stanovisek má tajemník Výboru pro řízení KB povinnost provést jejich vyhodnocení a výsledné rozhodnutí posléze distribuuje všem členům Výboru pro řízení KB. Materiál je považován za schválený, pokud s ním vysloví ve stanovené lhůtě souhlas nadpoloviční většina všech členů Výboru pro řízení KB.

3. Usnesení k takto schválenému materiálu bude mít stejnou platnost, jako by bylo přijato na zasedání Výboru pro řízení KB.

4. Na nejbližším zasedání Výboru pro řízení KB je místopředseda Výboru pro řízení KB nebo pověřený člen povinen informovat Výbor pro řízení KB o všech usneseních přijatých „per rollam“ v období mezi zasedáními Výboru pro řízení KB.

Článek 5
Příprava a předkládání materiálů na zasedání Výboru pro řízení KB

1. Materiály pro zasedání Výboru pro řízení KB se předkládají tajemníkovi Výboru pro řízení KB nejméně dva pracovní dny před plánovaným zasedáním Výboru pro řízení KB, nejde-li o mimořádné zasedání Výboru pro řízení KB, v takovém případě je možné materiály předložit až v průběhu mimořádného zasedání Výboru pro řízení KB.

2. Materiály jsou tajemníkovi Výboru pro řízení KB předkládány buď v písemné podobě v jednom výtisku, nebo v elektronické podobě.

Politika bezpečnostních rolí

Část I
Statut Manažera kybernetické bezpečnosti

Článek 1
Postavení Manažera KB

1. K zajištění a výkonu agendy kybernetické bezpečnosti na UPCE je zřízena role Manažera KB.
2. Manažer KB je podřízen rektorovi UPCE.
3. Manažera KB určuje rektor UPCE.
4. Manažer KB zajišťuje úkony vyplývající z povinností role Manažera KB dle Zákona a prováděcích právních předpisů.
5. Manažer KB nesmí být pověřen výkonem rolí odpovědných za provoz technických aktiv regulované služby. Role Manažera KB není slučitelná s rolemi odpovědnými za provoz ICT (informační a komunikační technologie) a s dalšími provozními a řídícími rolemi.
6. Rektor zajistí zastupitelnost Manažera KB. V případě dlouhodobé nepřítomnosti Manažera KB pověří rektor dočasně jeho zastupováním jiného vhodného zaměstnance.

Článek 2
Práva a povinnosti Manažera KB

1. Manažer KB odpovídá za:
   a) registraci regulované služby podle § 4 Zákona, změny a zrušení registrace regulované služby,
   b) za vedení seznamu aktiv UPCE,
   c) řízení SŘBI od průzkumu a analýz, přes průběžné testování prevence až po eliminaci následků a vyhodnocení „úspěšných“ kybernetických incidentů na UPCE,
   d) pravidelný reporting pro vrcholné vedení UPCE o
      - činnostech vyplývajících z rozsahu jeho odpovědnosti,
      - stavu SŘBI,
   e) pravidelnou komunikaci s vrcholným vedením UPCE,
   f) koordinaci a podílení se na procesu řízení aktiv a rizik; průběžně analyzuje vývoj SŘBI a vyhodnocuje identifikovaná kybernetická rizika, detekované KBU a odhalené KBI a předkládá o nich zprávu, jejímž obsahem jsou i návrhy na zmírnění nepřijatelných rizik a návrhy na změnu priorit bezpečnostních projektů Výboru pro řízení KB,

g) předkládání zpráv o hodnocení aktiv a rizik, plánu zvládání rizik a prohlášení o aplikovatelnosti Výboru pro řízení KB minimálně 1x ročně,
h) poskytování pokynů pro zajištění bezpečnosti informací při sjednání, hodnocení, výběru, řízení a ukončení dodavatelských vztahů,
i) komunikaci s Vládním nebo Národním CERT,
j) koordinaci řízení KBI,
k) vyhodnocování vhodnosti a účinnosti bezpečnostních opatření.

2. Manažer KB je oprávněn stanovit:
   a) rozsah a hranice systému zajišťování kybernetické bezpečnosti (s ohledem na aktiva a organizační bezpečnost), ve kterém určí, kterých organizačních částí a technických prvků se systém zajišťování kybernetické bezpečnosti týká,
   b) jednotnou metodiku pro identifikaci a hodnocení aktiv a metodiku pro stanovení kritérií pro přijatelnost rizik,
   c) cíle strategii (plán) řízení kontinuity další činnosti pro oblast kybernetické bezpečnosti,
   d) provozní pravidla a postupy systému zajišťování kybernetické bezpečnosti,
   e) plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik včetně určení osoby zajišťující prosazování bezpečnostních opatření.

3. Podílí se na schvalování závazných vnitřních norem UPCE pro výběr, unifikaci a systemizaci technických a programových prostředků informačních technologií UPCE.

4. V případě zavádění nových informačních systémů, které by mohly mít vliv na kybernetickou bezpečnost UPCE, Manažer KB:
   a) na požádání poskytuje součinnost,
   b) je informován o zkušebním a ověřovacím provozu a zátěžových testech,
   c) podílí se na přípravě smluvní dokumentace.

5. Kontroluje po věcné stránce formulaci zadávacích požadavků veřejných zakázek (včetně veřejných zakázek malého rozsahu) na výstavbu a modernizaci informačních a komunikačních systémů UPCE, či na pořízení dodávek či služeb, jejichž komponenty mohou mít vliv na kybernetickou bezpečnost UPCE, z hlediska standardů kybernetické bezpečnosti a poskytuje součinnost zadavateli v zadávacích řízeních týkajících se vyřešení otázek souvisejících s kybernetickou bezpečností.

6. Rozhoduje o realizaci bezpečnostního opatření na základě informací z monitorovacích a dohledových systémů, rozhodnutí Výboru pro řízení KB nebo Úřadu.

7. Zajišťuje zejména:
   a) detekci KBU, proces řešení KBU nebo KBI a rozhoduje o způsobu jejich řešení,
   b) zpracovávání zpráv o hodnocení aktiv a rizik a prohlášení o aplikovatelnosti, které obsahuje přehled zavedených bezpečnostních opatření,

c) u dodavatelů pravidelné hodnocení rizik, provádění kontrol zavedených bezpečnostních opatření u poskytovaných služeb a odstraňování zjištěných nedostatků,
d) aktualizaci systému zajišťování kybernetické bezpečnosti a příslušné dokumentace dle výsledků auditů nebo významných změn a vyhodnocení účinnosti bezpečnostních opatření,
e) aktualizaci zprávy o hodnocení aktiv a rizik, bezpečnostní politiky; plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí,
f) realizaci reaktivních opatření vydaných Úřadem,
g) součinnost při provádění kontrolních auditů prováděných Úřadem.

8. Navrhuje změny strategie kybernetické bezpečnosti UPCE a bezpečnostní politiky SŘBI.

9. Vypracovává plán rozvoje bezpečnostního povědomí a s tímto plánem seznamuje Výbor pro řízení KB.

10. Koordinuje opatření ke zvýšení bezpečnostního povědomí na UPCE včetně školení a cvičení kybernetické bezpečnosti. Odpovídá za stanovení pravidel pro dodavatele, která zohledňují potřeby SŘBI.

11. Manažer KB je oprávněn vyžadovat:
    a) od Výboru pro řízení 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,
        - určení osob pro výkon rolí Garantů aktiv,
        - provedení základní identifikace aktiv.
    b) od Garanta aktiva:
        - podklady pro evidenci podmínek provozování a obnovy aktiva,
        - předložení seznamu aktuálních hrozeb, zranitelností a identifikovaných rizik,
        - ohodnocení přijatelnosti rizik,
        - způsob zajištění bezpečnostních parametrů (úrovní) prostřednictvím SLA (Service Level Agreement),
        - identifikaci souvisejících podpůrných aktiv a jejich rizik,
        - vyhodnocení účinnosti bezpečnostních opatření.

12. Při porušení stanovených bezpečnostních zásad a pravidel zaměstnancem UPCE je příslušný vedoucí zaměstnanec ve spolupráci s Manažerem kybernetické bezpečnosti povinen řádně vyšetřit všechny okolnosti a příčiny, které k němu vedly, vyhodnotit konkrétní dopady na bezpečnostní situaci a přijmout účinná opatření k zamezení jeho možného opakování, jakož i zajistit vymáhání případné vzniklé škody a postih odpovědné osoby. Obdobný postup se použije v případě externích fyzických a právnických osob.

Část II
Statut Architekta kybernetické bezpečnosti

Článek 1
Postavení Architekta Kybernetické bezpečnosti

1. Architekt kybernetické bezpečnosti (dále jen „Architekt KB“) vykonává roli v souladu se Zákonem a prováděcími právními předpisy, odpovídá za plnění vymezených úkolů v rozsahu jemu svěřené bezpečnostní role.
2. Architekta KB navrhuje Manažer KB a určuje rektor UPCE.
3. Bezpečnostní role Architekta KB je neslučitelná s rolemi odpovědnými za provoz ICT.
4. Rektor zajistí zastupitelnost Architekta KB. V případě dlouhodobé nepřítomnosti Architekta KB pověří rektor dočasně jeho zastupováním jiného vhodného zaměstnance.

Článek 2
Odpovědnosti a pravomoci Architekta KB

1. Architekt KB je osoba odpovědná za:
   a) zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura regulované služby,
   b) stanovení, dokumentování, údržbu a stálý rozvoj vhodné bezpečné architektury regulovaných služeb podle aktuální dobré praxe, tj. porovnávání shody navržených bezpečnostních opatření s požadavky legislativy, technickými a průmyslovými standardy a strategií a potřebami UPCE.

2. Hlavní úlohou Architekta KB je na základě schválené strategie a cílů kybernetické bezpečnosti bezpečnostní politiky UPCE navrhnout a metodicky dozorovat implementace odpovídajících bezpečnostních opatření na UPCE a existující opatření průběžně analyzovat a s výsledky seznamovat Manažera KB a Výbor pro řízení KB.

3. Architekt KB samostatně zajišťuje:
   a) návrhy a realizaci procesů hodnocení a evidence aktiv a rizik kybernetické bezpečnosti na základě podkladů předložených Garanty aktiv a Manažerem KB,
   b) identifikaci možných postupů pro zajištění požadované míry kybernetické bezpečnosti v souladu se strategií UPCE,
   c) model architektury kybernetické a informační bezpečnosti UPCE (procesní model, aplikační architektura, technologie apod.),
   d) identifikaci možných postupů a opatření pro redukci identifikovaných rizik v souladu se strategií a architekturou kybernetické bezpečnosti, vlastnostmi aktiv, prostředí a riziky,
   e) zastupování UPCE v projektech implementace bezpečnostních opatření kybernetické bezpečnosti, pro zajištění souladu s architekturou kybernetické bezpečnosti UPCE, vlastnostmi aktiv, prostředí a riziky,
   f) společně s dalšími bezpečnostními rolemi pak:
      - spolupracuje na tvorbě vnitřních norem UPCE a standardů pro oblast informační a kybernetické bezpečnosti,

- spolupracuje na vytváření a aktualizaci katalogu hrozeb a zranitelností aktiv UPCE,
- spolupracuje na aktualizaci strategie kybernetické bezpečnosti a plánování v souladu se strategickými cíli UPCE,
- spolupracuje na definování klíčových projektů k naplnění bezpečnostní politiky a k cílovému stavu modelu architektury kybernetické bezpečnosti UPCE,
- poskytuje podporu implementace nových procesů v rozsahu organizace a zajištění přechodu na nové modely fungování informační a kybernetické bezpečnosti,
- zajišťuje implementační dohled vybraných opatření kybernetické bezpečnosti a jejich kompozici v architektuře kybernetické bezpečnosti UPCE,
- spolupracuje na procesech řešení KBU a KBI.

Část III
Statut Auditora kybernetické bezpečnosti

Článek 1
Postavení Auditora Kybernetické bezpečnosti

1. Auditor kybernetické bezpečnosti (dále jen „Auditor KB“) vykonává bezpečností roli na základě určení rektorem v souladu se Zákonem, prováděcími právními předpisy a podle principů interního auditu.

2. Role Auditora KB je neslučitelná s rolemi Výboru pro řízení KB a s jinými bezpečnostními rolemi. Role Auditora KB je dále neslučitelná s výkonem rolí odpovědných za provoz ICT. Je vykonávána nezávisle.

3. Hlavní úlohou Auditora KB je provádění auditů kybernetické bezpečnosti na UPCE. Zaručuje, že provedení auditu kybernetické bezpečnosti je nestranné.

Článek 2
Odpovědnosti a pravomoci Auditora KB

1. Auditor KB odpovídá za plnění vymezených úkolů v rozsahu svěřené bezpečnostní role:
   a) za provádění auditu kybernetické bezpečnosti,
   b) hodnocení správnosti a účinnosti zavedených bezpečnostních opatření.

2. Auditor KB má právo:
   a) přistupovat k informacím a získávat informace dle potřeb stanovených rozsahem auditu,
   b) podílet se na definici opatření pro odstranění zjištění, která jsou učiněna v rámci auditů,
   c) spolupracovat na vypracování a úpravě metodiky pro audity KB.

3. Auditor KB má povinnost:

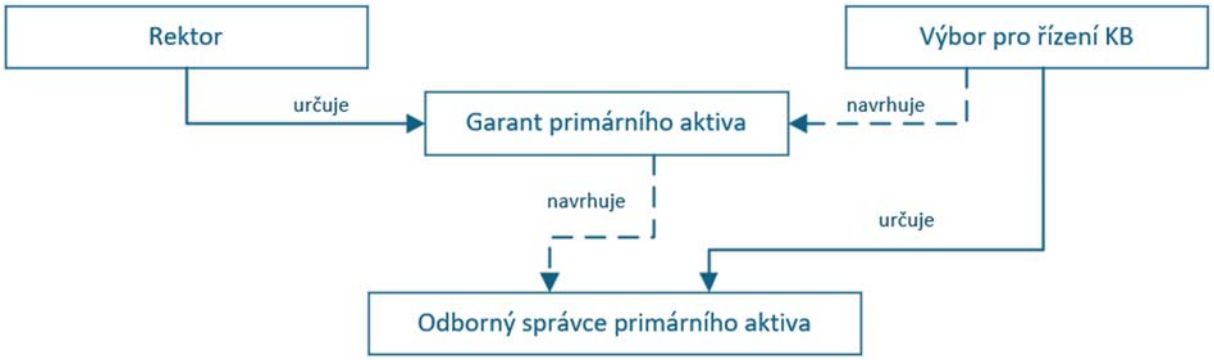
a) plánovat kybernetické bezpečnostní audity informačních a komunikačních systémů UPCE v souladu s principy interního auditu,
b) vést dokumentaci o průběhu auditu v souladu s principy interního auditu,
c) z jednotlivých auditů KB zpracovávat závěrečné auditní zprávy a spolu s návrhy opatření je předkládat Výboru pro řízení KB, Manažerovi KB a Garantovi primárního aktiva auditovaného systému. Výbor pro řízení KB projedná auditní zprávu a rozhodne o plánu realizace navržených nápravných opatření.

Část IV
Určení osob odpovědných za aktiva

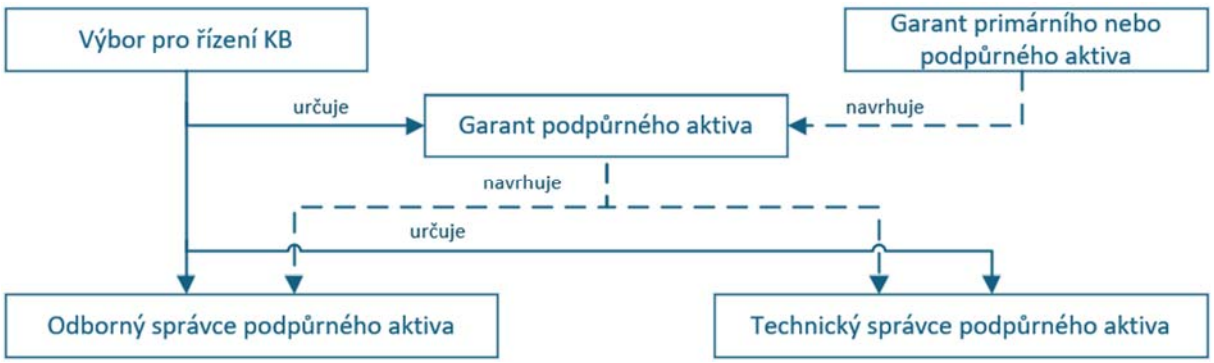
1. Proces určení osob odpovědných za aktiva je navržen tak, aby byla zajištěna jasná odpovědnost za řízení aktiv, oddělení odborných a technických kompetencí a účinný dohled nad bezpečností a provozem aktiv v celém jejich životním cyklu. Vztahy mezi jednotlivými rolemi jsou založeny na principu odpovědnosti, odborné nezávislosti a vzájemné spolupráce.

2. Určení odpovědných osob je dáno v závislosti na konkrétním typu aktiva, přičemž pro každý typ aktiva jsou jasně vymezeny odpovědnosti a role příslušných osob v souladu s touto směrnicí.

Obrázek č. 3: Určení osob odpovědných za primární aktivum



Obrázek č. 4: Určení osob odpovědných za podpůrné aktivum



Část V
Statut Garanta

Článek 1
Postavení Garanta

1. Garant je pověřen k zajištění rozvoje, použití a bezpečnosti aktiva.

2. Garant je bezpečnostní rolí, která má hlavní a nejucelenější přehled o tom, jak je s daným aktivem a informacemi v něm nakládáno ve smyslu řízení procesů a informací. Pro výkon své funkce musí být Garant dobře obeznámen s procesy UPCE.

3. Garant vykonává roli v souladu se Zákonem a prováděcími právními předpisy, odpovídá za plnění vymezených úkolů v rozsahu jemu svěřené bezpečnostní role.

4. Garanta primárního aktiva navrhuje Výbor pro řízení KB a určuje rektor UPCE.

5. Garanta podpůrného aktiva navrhuje Garant primárního aktiva nebo Garant jiného podpůrného aktiva a určuje jej Výbor pro řízení KB.

6. Garant primárního aktiva je oprávněn navrhovat osobu do role Odborného správce primárního aktiva. Role Technického správce primárního aktiva se nestanovuje, neboť není pro dané aktivum relevantní.

7. Garant podpůrného aktiva je oprávněn navrhovat osoby do role Odborného správce podpůrného aktiva a Technického správce podpůrného aktiva.

8. Garant spolupracuje a řídí osoby v rolích odborného správce aktiva a technického správce aktiva a spolupracuje s ostatními osobami zastávajícími bezpečnostní role.

9. Garant primárního aktiva aktivum přímo nespravuje. Jeho rolí je přijímat podněty v oblasti řízení rizik, řízení změn, plánování odstávek a dalších procesů, které mohou mít na primární aktivum dopad. Dále navrhuje rozšíření nebo změnu účelu aktiva a poskytuje ostatním bezpečnostním rolím popis aktiva za účelem zajištění kvality procesů UPCE, které jsou tímto aktivem podporovány.

10. Garant primárního aktiva vystupuje jako zástupce primárního aktiva při strategických rozhodnutích vedení UPCE a při provádění auditů.

Článek 2
Odpovědnosti a pravomoci Garanta

1. Garant primárního aktiva odpovídá za to, že je aktivum řádně řízeno, chráněno a rozvíjeno. Stanovuje jeho účel, význam a strategické cíle, zejména ve vztahu k plnění poslání UPCE, právním povinnostem a poskytovaným regulovaným službám.

2. Garant podpůrného aktiva odpovídá za soulad podpůrného aktiva s požadavky garantů ostatních aktiv, které aktivum podporuje. Stanovuje jeho účel, význam a strategii využití tak, aby podpůrné aktivum efektivně a bezpečně podporovalo jedno nebo více aktiv.

3. Garant má následující odpovědnosti a pravomoci:
   a) odpovídá za zajištění rozvoje, použití a bezpečnost jemu svěřeného aktiva,
   b) plní požadavky SŘBI týkající se svěřeného aktiva v souladu s právními předpisy a interními pravidly, do jeho kompetence spadá zejména oblast organizačních opatření a aktivem podporované procesy,
   c) rozhoduje o změnách aktiva z hlediska funkčnosti, bezpečnosti a rizik, jeho vyřazení nebo výměně,
   d) určuje klasifikaci aktiva, vede seznam podporovaných procesů a posuzuje jeho další parametry,
   e) schvaluje bezpečnostní dokumentaci aktiva,
   f) v oblasti bezpečnostní dokumentace se Garant mimo jiné podílí na identifikaci a hodnocení rizik aktiva i jeho podpůrných aktiv a předkládá manažerovi KB návrh přijatelnosti či nepřijatelnosti identifikovaných kybernetických bezpečnostních rizik a nápravných opatření,
   g) Garant spolupracuje při řešení KBU nebo KBI s Manažerem KB, včetně implementace reaktivních opatření dle pokynů Manažera KB nebo Výboru pro řízení KB,
   h) Garant v předstihu informuje o plánovaných odstávkách nebo úpravách svěřeného aktiva.

4. Garant je oprávněn:
   a) vyžadovat od Odborného správce a Technického správce:
      - veškeré potřebné informace o stavu aktiva, aktualizované hodnocení hrozeb, zranitelností, rizik a plány obnovy a kontinuity,
      - zajištění úplnosti daného aktiva a ověřovat, zda aktivum odpovídá jeho požadavkům,
   b) pozastavit využívání aktiva při významných rizicích,
   c) být informován o rozhodnutích Výboru pro řízení KB týkajících se svěřeného aktiva, a to zejména v případech rozhodnutí o neschválení Garantem navržené přijatelnosti či nepřijatelnosti identifikovaných kybernetických bezpečnostních rizik,
   d) vyžadovat od Auditora KB závěrečné zprávy z auditu svěřeného aktiva,
   e) podat podnět k provedení auditu nebo kontroly souvisejících aktiv předsedovi Výboru pro řízení KB v případě podezření na porušení pravidel.

Část VI
Statut Odborného správce

Článek 1
Postavení Odborného správce

1. Odborného správce (primárního nebo podpůrného aktiva) navrhuje Garant a určuje jej Výbor pro řízení KB.
2. Odborný správce je odborníkem na funkční, procesní a obsahovou stránku aktiva.
3. Odborný správce je odpovědný Garantovi. V případě podpůrného aktiva je jeho postavení rovnocenné postavení Technického správce.
4. Odborný správce zajišťuje požadavky Garanta na funkční a procesní požadavky vztahující se k danému aktivu.
5. Odborný správce je klíčovou osobou při posuzování dopadů změn aktiva na jeho funkčnost a na informace poskytované tímto aktivem.
6. Odborný správce spolupracuje s ostatními osobami zastávajícími bezpečnostní role na UPCE.

Článek 2
Odpovědnosti a pravomoci Odborného správce

1. Odborný správce odpovídá za:
   a) věcnou a obsahovou správnost daného aktiva, tj. aby aktivum plnilo svou funkci a odpovídalo požadavkům garanta, potřebám uživatelů a procesů UPCE,
   b) návrh funkčních a bezpečnostních požadavků,
   c) posuzování a hodnocení rizik z hlediska provozních a procesních dopadů,
   d) odbornou podporu Garantovi a Technickému správci při snižování rizik,
   e) informování Garanta o rozsahu přístupů nebo způsobu využívání aktiva,
   f) spolupráci s Technickým správcem a při hodnocení zranitelností, hrozeb, řešení incidentů a změn,
   g) vedení a aktualizaci:
      - odborného popisu aktiva (účel, funkce, podporované procesy, vazby, obsah),
      - záznamů o změnách aktiva,
   h) Garantovi a Manažerovi KB hlásí nestandardní projevy v chování aktiva za účelem detekce KBU a KBI,
   i) zapojení do auditů a kontrol.

2. Odborný správce je oprávněn:
   a) navrhovat funkční a procesní změny aktiva,
   b) vyžadovat od Technického správce technické informace potřebné k posouzení stavu aktiva a aktualizaci plánů obnovy a kontinuity,
   c) iniciovat řešení odborných nesouladů nebo rizik,
   d) posuzovat návrhy na technické změny z pohledu funkčnosti a obsahu.

Část VII
Statut Technického správce

Článek 1
Postavení Technického správce

1. Technického správce navrhuje Garant podpůrného aktiva a určuje jej Výbor pro řízení KB.
2. Technický správce je odborníkem na provozní a technickou stránku aktiva.
3. Technický správce je odpovědný Garantovi a jeho postavení je rovnocenné postavení Odborného správce.
4. Technický správce zajišťuje požadavky Garanta na funkční, procesní a bezpečnostní požadavky na aktivum.
5. Technický správce spolupracuje s ostatními osobami zastávajícími bezpečnostní role na UPCE.

Článek 2
Odpovědnosti a pravomoci Technického správce

1. Technický správce odpovídá za:
   a) technickou správu, podporu a implementaci bezpečnostních opatření pro dané aktivum,
   b) provoz, dostupnost, integritu, monitoring, údržbu a technické zabezpečení aktiva,
   c) správu přístupů, logování, zálohování, aktualizace, konfigurace, funkční a bezpečnostní testování v souladu s požadavky garantů a platných standardů.
   d) vedení a aktualizaci:
      - plánů obnovy a kontinuity aktiva,
      - technické dokumentace, záznamů o změnách aktiva a testech obnovy,
      - seznamu služeb, které aktivum poskytuje a potřebuje ke svému provozu,
      - zranitelností a hrozeb dle přílohy č. 3 vyhlášky č. 409/2025 Sb. jako podklad pro analýzu rizik aktiva, s aktualizací minimálně 1x ročně.
   e) poskytování dokumentace, technických údajů a záznamů Garantovi a Odbornému správci,
   f) Garantovi a Manažerovi KB hlásí nestandardní projevy v technickém chování aktiva za účelem detekce KBU a KBI,
   g) účast na auditech a bezpečnostních kontrolách.

2. Technický správce je oprávněn:
   a) provádět technické zásahy a konfigurace za účelem bezpečnosti aktiva a v souladu s požadavky Garanta,
   b) navrhovat technická bezpečnostní opatření a vylepšení,
   c) dočasně omezit provoz aktiva na dobu nezbytně nutnou při technických nebo bezpečnostních rizicích nebo při aktualizacích (po předchozím informování Garanta a Odborného správce),
   d) žádat doplnění odborných nebo organizačních informací od Garanta nebo od Odborného správce.

Politika řízení bezpečnostní politiky a bezpečnostní dokumentace

1. UPCE v rámci řízení bezpečnostní politiky a bezpečnostní dokumentace:
   a) stanoví bezpečnostní politiku ve vztahu k řízení kybernetické bezpečnosti a vede relevantní bezpečnostní politiku a bezpečnostní dokumentaci k opatřením uvedeným v § 3 až 27 vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností,
   b) dodržuje pravidla a postupy stanovení v bezpečnostní politice a bezpečností dokumentaci podle písmene a),
   c) pravidelně přezkoumává bezpečností politiku a bezpečnostní dokumentaci, zajistí jejich aktuálnost a zohlední jejich relevantní oblasti v provozních pravidlech a postupech a další dokumentaci.

2. Za pravidelnou kontrolu a revizi, resp. aktualizaci bezpečnostní politiky, bezpečnostní dokumentace a zohlednění jejich relevantních oblastí v provozní dokumentaci odpovídá Manažer KB.

3. Bezpečnostní politika a bezpečnostní dokumentace podléhá schválení Výboru pro řízení KB.

4. Bezpečnostní dokumentací se rozumí relevantní části této Směrnice, definice rozsahu SŘBI, samostatně zpracovaná bezpečnostní dokumentace ke každé regulované službě, bezpečnostní politiky a zprávy z auditu SŘBI.

5. Bezpečnostní dokumentace musí být kontrolována a pravidelně revidována (minimálně 1x ročně), revize však může být také provedena mimořádně na základě výsledků bezpečnostního auditu nebo jako důsledek významné změny bezpečnostních potřeb UPCE vyvolané např. změnou právní úpravy nebo úpravou interních procesů na UPCE.

6. Bezpečnostní politika a bezpečnostní dokumentace musí být řízeny tak, aby byly:
   a) dostupné v elektronické nebo listinné podobě,
   b) komunikovány v rámci UPCE,
   c) přiměřeně dostupné dotčeným stranám,
   d) chráněny z pohledu důvěrnosti, integrity a dostupnosti,
   e) vedeny tak, aby informace v nich obsažené byly úplné, čitelné, správné, snadno identifikovatelné a vyhledatelné.

7. Za umístění aktuální bezpečnostní politiky a bezpečnostní dokumentace odpovídá Manažer KB.