|  |  |
| --- | --- |
|  |  |
| **Metodický pokyn poskytovatelům zdravotních služeb ke kybernetické bezpečnosti****Příloha č. 1****Bezpečnostní politika informací Organizace (vzor)** |
| Pořadí revize | Provedené dne | Zpracoval | Schválil  |
| Verze 1.0 |  | Tomáš Bezouška, CISA kolektiv autorů | Ing. Martin Zeman |
| Verze 2.0 | 12.6.2019 | Tomáš Bezouška, CISA, Ing. Martin ŠvandaIng. Jiří Borej, CGEIT kolektiv autorů | Ing. Martin Zeman |

**Obsah**

[Obsah 2](#_Toc11182567)

[Seznam tabulek 3](#_Toc11182568)

[Seznam obrázků 3](#_Toc11182569)

[Seznam zkratek a pojmů 3](#_Toc11182570)

[Preambule 5](#_Toc11182571)

[1 Úvodní ustanovení 6](#_Toc11182572)

[1.1 Závaznost 6](#_Toc11182573)

[1.2 Rozsah Bezpečnostní politiky informací 6](#_Toc11182574)

[1.3 Základní charakteristika bezpečnosti informací 7](#_Toc11182575)

[1.4 Cíl bezpečnosti informací 7](#_Toc11182576)

[1.5 Revize Bezpečnostní politiky informací 7](#_Toc11182577)

[1.6 Uplatnitelnost Bezpečnostní politiky 7](#_Toc11182578)

[2 Cíle a zásady bezpečnosti informací 8](#_Toc11182579)

[3 Legislativní rámec 9](#_Toc11182580)

[3.1 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti 9](#_Toc11182581)

[3.2 Zákon č. 365/2000 Sb., o IS veřejné správy 10](#_Toc11182582)

[3.3 Zákon č. 240/2000 Sb., o krizovém řízení 10](#_Toc11182583)

[3.4 Nařízení vlády č. 315/2014 Sb., o kritériích pro určení prvku kritické infrastruktury 10](#_Toc11182584)

[3.5 Systém řízení bezpečnosti informací 10](#_Toc11182585)

[4 Rozsah systému řízení bezpečnosti informací 11](#_Toc11182586)

[4.1 Způsoby stanovení 11](#_Toc11182587)

[4.2 Stanovení bezpečnostního perimetru 11](#_Toc11182588)

[4.3 Identifikace primárních aktiv 12](#_Toc11182589)

[4.4 Identifikace podpůrných aktiv 12](#_Toc11182590)

[5 Systém řízení bezpečnosti informací 13](#_Toc11182591)

[5.1 Výbor pro řízení kybernetické bezpečnosti 15](#_Toc11182592)

[5.2 Architekt kybernetické bezpečnosti 17](#_Toc11182593)

[5.3 Auditor kybernetické bezpečnosti 18](#_Toc11182594)

[5.4 Garant aktiva 20](#_Toc11182595)

[5.5 RACI matice zákonných bezpečnostních rolí 21](#_Toc11182596)

[5.6 Vyškolení rolí kybernetické bezpečnosti 22](#_Toc11182597)

[6 Procesy a zásady řízení bezpečnosti informací 23](#_Toc11182598)

[6.1 Klasifikace a řízení informačních aktiv 23](#_Toc11182599)

[6.2 Kritéria hodnocení rizik 23](#_Toc11182600)

[6.3 Řízení lidských zdrojů 23](#_Toc11182601)

[6.4 Řízení fyzické bezpečnosti 24](#_Toc11182602)

[6.5 Řízení preventivních a nápravných opatření 25](#_Toc11182603)

[6.6 Řízení bezpečnosti komunikací a provozu 25](#_Toc11182604)

[6.7 Řízení přístupu 25](#_Toc11182605)

[6.8 Vývoj a údržba systémů 25](#_Toc11182606)

[6.9 Řízení dodavatelů 26](#_Toc11182607)

[6.10 Řízení kontinuity činností 27](#_Toc11182608)

[6.11 Soulad s požadavky na ochranu informací 27](#_Toc11182609)

[6.12 Odpovědnosti pro bezpečnost informací 27](#_Toc11182610)

[6.13 Přezkoumávání a audity 28](#_Toc11182611)

[7 Struktura bezpečnostní dokumentace 29](#_Toc11182612)

[7.1 Obecná bezpečnostní dokumentace 29](#_Toc11182613)

[7.2 Bezpečnostní dokumentace 29](#_Toc11182614)

[8 Závěrečná ustanovení 31](#_Toc11182615)

## Seznam tabulek

[Tabulka 2 – Matice rolí 21](#_Toc11182616)

## Seznam obrázků

[**Obrázek 1** – Hierarchie bezpečnostních rolí 14](#_Toc11182617)

## Seznam zkratek a pojmů

| Zkratka | Význam |
| --- | --- |
| KB | Kybernetická bezpečnost |
| ZKB |  Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů |
| VKB | Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) |
| ISMS | Systém řízení bezpečnosti informací |
| NBÚ  | Národní bezpečnostní úřad |
| Sb. | Sbírka zákonů České republiky |
| ČR | Česká republika |
| KII  | kritická informační infrastruktura |
| VIS | významný informační systém |
| NCKB | Národní centrum kybernetické bezpečnosti |
| RACI | Matice odpovědností |
| CERT | Computer Emergency Response Team |
| IT  | Informační technologie |
| SOC | resortní dohledové centrum |
| NÚKIB |  Národní úřad pro kybernetickou a informační bezpečnost |
| ISO | Mezinárodní organizace pro standardizaci |
| IEC | International Electrotechnical Commission  |

# Preambule

**Závazek vedení**

Organizace prohlašuje, že podporuje ustavení, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování systému řízení bezpečnosti informací v Organizaci a bude dohlížet na dodržování tohoto systému, bude propagovat význam jeho zavedení, udržování a zlepšování a bude ve spolupráci s Výborem pro řízení kybernetické bezpečnosti a vedoucími zaměstnanci Organizace dbát na plnění povinností z něj vyplývajících všemi zaměstnanci.

S ohledem na maximální zabezpečení informací je prováděno periodické, dokumentované monitorování a vyhodnocování bezpečnostních rizik a incidentů. Je zajišťováno neustálé zlepšování bezpečnosti informací (tj. zabezpečení včasné dostupnosti informací, zamezení jejich modifikace, zneužití a ztráty) v souladu s obecně závaznými právními a interními předpisy a smluvními požadavky.

# Úvodní ustanovení

Organizace byla zřízena doplnit. Působnost Organizace je vymezena doplnit a zahrnuje následující odpovědnosti a kompetence.

* doplnit.

Organizace vyhlašuje zásady bezpečnosti informací platné pro všechny své zaměstnance, externí spolupracovníky a dodavatele (viz dále kapitola 1.1 Závaznost).

Tato Bezpečnostní politika informací je vypracovávána v souladu s požadavky definovanými v ZKB a jeho prováděcích předpisech, tj.:

* vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, a náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, v aktuálním znění,
* nařízení vlády č. 432/2010 Sb, o kritériích pro určení prvku kritické infrastruktury ve znění pozdějších předpisů a
* vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

Tato Bezpečnostní politika informací musí být vždy v souladu s Bezpečnostní politikou informací MZ ČR.

## Závaznost

Povinnost řídit se ZKB má orgán nebo osoba uvedená v § 3 ZKB a tato osoba spolupracuje a postupuje alespoň v rozsahu stanoveném v ZKB. Organizace je v souladu s ustanovením §3 písm. f) určena jako správce a provozovatel informačního systému základní služby.

Organizace jakožto správce a provozovatel informačního systému základní služby implementuje alespoň v rozsahu stanoveném v ZKB Systém řízení bezpečnosti informací (ISMS). NÚKIB kontroluje soulad Systému řízení bezpečnosti informací (ISMS) Organizace se zákonem.

Tato politika je závazná pro všechny zaměstnance Organizace.

## Rozsah Bezpečnostní politiky informací

K zajištění bezpečnosti informací a podpory bezpečnosti informací se Organizace řídí touto politikou:

1. popisuje a vysvětluje zajištění bezpečnosti informací,
2. stanovují bezpečnostní cíle,
3. stanovuje rozsah a důležitost bezpečnosti informací,
4. uvádí stručný výklad základních bezpečnostních zásad,
5. stanovují kritéria, kterými bude hodnoceno riziko, a definuje struktura hodnocení rizik.

Problematika bezpečnosti informací pokrývá celou strukturu Organizace ve všech lokalitách jejího působení, včetně spolupracujících organizací, které přichází do styku se zabezpečenými informacemi Organizace. Bezpečnost informací se dotýká všech identifikovaných informačních aktiv Organizace, a to v míře a rozsahu odpovídajícím významu daného aktiva.

## Základní charakteristika bezpečnosti informací

Bezpečnost informací je charakterizována jako zachování důvěrnosti, integrity a dostupnosti informací, přičemž:

1. **důvěrnost** je zajištění toho, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům,
2. **integrita** je zabezpečení přesnosti a úplnosti informace a metod jejího zpracování,
3. **dostupnost** je zajištění toho, že jsou informace je přístupná a použitelná na žádost oprávněného jednotlivce, entity nebo procesu.

## Cíl bezpečnosti informací

Bezpečnostním cílem spojeným s bezpečností informací v Organizaci je zajištění dostupnosti informačních aktiv jen oprávněným osobám, správnosti a kompletnosti informací, důvěrnosti a bezpečnosti jejich zpracování a ochrany informací proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, proti neoprávněnému přístupu, změnám nebo šíření, a to v souladu se zákony a jinými právními předpisy ČR.

## Revize Bezpečnostní politiky informací

Revize Bezpečnostní politiky informací provádí Organizace nejméně jednou ročně. Za provedení revize dokumentu Bezpečnostní politiky informací odpovídá Manažer kybernetické bezpečnosti, finální verzi dokumentu schvaluje Výbor pro řízení kybernetické bezpečnosti.

Záměrem Organizace je udržovat přiměřenou ochranu informačních aktiv, včetně aktiv podpůrných. Z důvodu zachování právní jistoty orgánů a osob je potřebné jednotlivé komponenty bezpečnostních opatření konkretizovat v souladu se zákony a jinými právními předpisy ČR v rámci řídící dokumentace zavedeného Systému řízení bezpečnosti informací.

## Uplatnitelnost Bezpečnostní politiky

Bezpečnost informací a kybernetická bezpečnost, jako její významná podmnožina, je v oblasti zdravotnictví s ohledem na velké množství a četnost zpracování citlivých informací a dat jedním ze zásadních témat, jejichž význam s postupující elektronizací zdravotnictví dále poroste.

Organizace touto Bezpečnostní politikou informací deklaruje zájem o plošné řešení této problematiky. Bezpečnostní politika informací byla proto zpracována jako vrcholový dokument Organizace, a spolu s navazující bezpečnostní dokumentací, zahrnující strategické dokumenty, politiky a metodiky pro jednotlivé dílčí oblasti, tvoří páteř systému řízení bezpečnosti informací Organizace.

# Cíle a zásady bezpečnosti informací

Zaměstnanci Organizace v rámci dodržování bezpečnosti informací zajišťují:

1. ochranu práv a svobod jednotlivců, zejména právo na soukromí uznané v článku 7 Úmluvy o ochraně lidských práv a základních svobod, usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ,
2. ochranu údajů týkajících se jednotlivých občanů, organizací nebo malých organizací, spojenou s povinností mlčenlivosti podle zvláštního zákona[[1]](#footnote-2),
3. ochranu osobních údajů a citlivých údajů podle zvláštního zákona,
4. ochranu skutečností, jejichž zneužití by mohlo vést k ohrožení života, zdraví, majetku, životního prostředí nebo podnikatelského zájmu právnické osoby nebo fyzické osoby vykonávající podnikatelskou činnost podle zvláštních právních předpisů,
5. ochranu osobnosti podle zvláštního zákona,
6. ochranu prostředků a dat pro vytváření zaručeného elektronického podpisu podle zvláštního zákona,
7. ochranu obchodního tajemství podle zvláštního právního předpisu a obsahu smluv obchodně závazkových vztahů, pokud se k tomu v uzavřené smlouvě dotčená Organizace zavázala,
8. ochranu listovního tajemství atd.

Organizace podporuje stanovené cíle bezpečnosti informací. Organizace vyjadřuje touto Bezpečnostní politikou informací svoji strategii trvalého zajišťování bezpečnosti informací jako nedílné součásti vlastních řídících procesů.

# Legislativní rámec

Kybernetická bezpečnost je dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, souhrn úkonů a bezpečnostních opatření, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací (dle zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů) v kybernetickém prostoru.

Zajištění provozní bezpečnosti je jednou z klíčových priorit Organizace v souladu se strategickým řízením a naplňováním požadavků a cílů Organizace, v podmínkách současné ale i připravované legislativy v oblasti kritické infrastruktury a kybernetické bezpečnosti.

## Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Věcným garantem zákona **č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB)** je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

Z pohledu Organizace jsou relevantními prováděcími právními předpisy k ZKB zejména:

* vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, a náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, v aktuálním znění,
* vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

### Vyhláška č. 82/2018Sb., o kybernetické bezpečnosti

 Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), definuje požadavky na bezpečnostní a technická opatření, bezpečnostní dokumentaci, hlášení bezpečnostních incidentů a provádění reaktivních opatření. Vyhláška vychází z:

* normy řady ISO/IEC 27000,
* knihovny ITIL,
* CRAMM a
* metodiky COBIT v.5 (ISACA)

### Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

Tato vyhláška na základě Směrnice Evropského parlamentu a Rady EU 2016/1148 upravuje odvětvová a dopadová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby podle § 22 odst. 1 ZKB.

## Relevantní evropská nařízení a směrnice

V oblasti bezpečnosti informací jsou vedle právních předpisů na národní úrovni relevantním zdrojem práva také nařízení a směrnice Evropského parlamentu a Rady (EU), které mají přímý dopad na nakládání s informacemi v Organizaci, případně jsou transponovány do odpovídající právní úpravy v českém právním řádu. Jedná se zejména o tyto směrnice a nařízení:

* směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, (směrnice NIS)
* nařízení Evropského parlamentu a Rady (EU) 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), (nařízení GDPR)
* nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, (nařízení eIDAS).

## Systém řízení bezpečnosti informací

Standardy určené k zavedení systému řízení bezpečnosti, z nichž mezi nejrozšířenější patří standardy řady ISO/IEC 27000 – Information Security Management System (dále jen ISMS), poskytují podporu pro ustavení, zavedení, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací. Z pohledu Organizace jsou za základní relevantní standardy považovány.

* ČSN EN ISO/IEC 27001 Systémy managementu bezpečnosti informací – Požadavky.
* ČSN EN ISO/IEC 27002 Soubor postupů pro opatření bezpečnosti informací.
* ČSN EN ISO 27799 Zdravotnická informatika - Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002.

ISMS je jeden ze základních kamenů, na kterém stojí efektivita a kvalita kybernetické bezpečnosti Organizace.

# Rozsah systému řízení bezpečnosti informací

## Stanovení rozsahu SŘBI

Rozsah systému řízení bezpečnosti informací byl s ohledem na stávající kapacitní možnosti Organizace zúžen pouze na ty systémy, ke kterým se váží povinnosti dané zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcích předpisů.

V průběhů implementace ZKB může dojít k zahrnutí i dalších prvků, u kterých je řízení bezpečnosti informací potřebné nikoli jako důsledek povinností uložených ZKB a jeho prováděcích předpisů, ale z důvodů vyplývajících z potřeb Organizace. Především podpůrná aktiva, která mohou být sdílená mezi různými informačními a komunikačními systémy, budou do sytému řízení bezpečnosti informací včleňována postupně na základě revizí relevantních částí řídící dokumentace.

### Primární aktiva

Za primární aktivum Organizace jsou v rámci stanovení počátečního rozsahu systému řízení bezpečnosti informací považovány všechny soubory informací nezbytné pro zajištění poskytování základní služby, respektive všechny informační systémy odpovídající této charakteristice.

### Podpůrná aktiva

Za podpůrné aktivum jsou v rámci stanovení počátečního rozsahu systému řízení bezpečnosti informací považována všechna technická zařízení, která jsou nezbytná pro provoz informačních systémů zajišťujících dostupnost, integritu a důvěrnost identifikovaných primárních aktiv Organizace.

## Stanovení bezpečnostního perimetru

Hlavní zásady stanovení bezpečnostního perimetru:

* Vně vymezeného rozsahu perimetru nesmí zůstat žádná aktiva ani opatření, jejichž narušení by mohlo způsobit narušení kteréhokoliv požadovaného parametru aktiv (dostupnost, integrita, důvěrnost), jež jsou předmětem ochrany dle ZKB.
* Musí být naplněn požadavek ZKB zajistit kybernetickou bezpečnost pro daná aktiva tak, že narušení jakéhokoliv systému, jehož je organizace správcem či provozovatelem, stojícího vně bezpečnostního perimetru, nemůže způsobit narušení bezpečnosti informací chráněného aktiva stojícího dle definice uvnitř perimetru.
* Každý systém, jehož je organizace provozovatelem a jehož narušení může přímo způsobit narušení bezpečnosti informací chráněného aktiva, musí být zahrnut v perimetru.
* Z organizačních útvarů musí do bezpečnostního perimetru být zahrnuty všechny útvary, jejichž pracovníci mohou, z hlediska svých oprávnění vůči systémům zahrnutým v bezpečnostním perimetru, svým chováním ovlivnit bezpečnost informací chráněných aktiv, a to i nepřímo prostřednictvím jejich vlivu na bezpečnost informací v podpůrných aktivech.
* Aktiva vlastněná, spravovaná či provozovaná třetími stranami, která mohou ovlivnit bezpečnost informací chráněného aktiva, musejí být zahrnuta v perimetru a vztahy s vlastníkem, správcem či provozovatelem takových aktiv musí být upraveny tak, aby respektovaly bezpečnostní požadavky a pravidla. Vztahy mezi aktivy nejsou vztahy dodavatelsko-odběratelskými ve smyslu § 7 VKB.

# Systém řízení bezpečnosti informací

Organizace řídí bezpečnost informací a koordinuje implementaci bezpečnostních opatření dle stanovené působnosti a odpovědnosti vedoucích zaměstnanců a dle ZKB a VKB.

K naplnění cílů Organizace v oblasti bezpečnosti informací je doplnit řídící akt ustanoven **Výbor pro řízení kybernetické bezpečnosti** (dále jen „Výbor“), který je vrcholovým koordinačním orgánem kybernetické bezpečnosti Organizace. Hierarchie bezpečnostních rolí je popsána v dále v kapitolách 5.1 až 5.4.



**Obrázek 1** – Hierarchie bezpečnostních rolí

K zabezpečení úkolů vyplývajících ze ZKB a VKB Organizace jakožto správce infromačních systémů Poskytovatele základní služby určí bezpečnostní role v souladu s těmito právními předpisy. Je ustavena role Manažera kybernetické bezpečnosti a Architekta kybernetické bezpečnosti, a to s cílem zajištění maximální koordinace všech činností při ochraně informačních aktiv a řešení kybernetické bezpečnosti.

Roli **Manažera kybernetické bezpečnosti** jmenuje doplnit, při jmenování musí respektovat zákonné požadavky na kvalifikaci Manažera kybernetické bezpečnosti. Manažer kybernetické bezpečnosti je oprávněn pověřit jiné osoby (s výjimkou Architekta kybernetické bezpečnosti a Auditora kybernetické bezpečnosti) výkonem konkrétních činností ve své kompetenci.

Roli **Architekta kybernetické bezpečnosti** jmenuje doplnit, při jmenování musí respektovat zákonné požadavky na kvalifikaci Architektakybernetické bezpečnosti. Architekt kybernetické bezpečnostije oprávněn pověřit jiné osoby (s výjimkou Manažera kybernetické bezpečnosti a Auditora kybernetické bezpečnosti) výkonem konkrétních činností ve své kompetenci.

Je ustavena role Auditora kybernetické bezpečnosti s cílem zajištění potřebných kontrolních mechanismů v oblasti ochrany informačních aktiv a řešení kybernetické bezpečnosti. Roli **Auditora kybernetické bezpečnosti** jmenuje doplnit, při jmenování musí respektovat zákonné požadavky na kvalifikaci auditora a ustanovení o neslučitelnosti rolí v rámci systému řízení kybernetické bezpečnosti.

Rovněž jsou Předsedou Výboru pro řízení kybernetické bezpečnosti určeni **Garanti aktiv** pro jednotlivá primární a podpůrná aktiva.

Úkoly a odpovědnosti Výboru a jednotlivých bezpečnostních rolí jsou popsány dále.

Provádění Bezpečnostní politiky zajišťují všichni vedoucí zaměstnanci Organizace dle stanovené působnosti a odpovědnosti. K naplňování úkolů souvisejících s bezpečností informací jsou zavázáni všichni zaměstnanci a dodavatelé Organizace.

## Výbor pro řízení kybernetické bezpečnosti

Výbor pro řízení kybernetické bezpečnosti (dále také jen „Výbor“) je ustaven doplnit ustavující akt. Výbor je pověřen celkovým řízením a rozvojem kybernetické bezpečnosti Organizace. Výbor zajišťuje činnosti spojené s celkovým řízením a rozvojem informačních systémů kritické informační infrastruktury a významných informačních systémů a významně se podílí na řízení a koordinaci činností spojených s kybernetickou bezpečností informačního systému Organizace jako celku.

Výbor je tvořen osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj systému řízení bezpečnosti informací a osobami významně se podílejícími na řízení a koordinaci činností spojených s kybernetickou bezpečností. Členem Výboru musí být vždy alespoň jeden zástupce vrcholového vedení Organizace nebo jím pověřená osoba a Manažer kybernetické bezpečnosti.

### Úkoly Výboru pro řízení kybernetické bezpečnosti

Výbor pro řízení kybernetické bezpečnosti zodpovídá zejména za:

* celkové řízení a rozvoj informačního systému kritické informační infrastruktury nebo významného informačního systému,
* tvorbu rámce kybernetické bezpečnosti a definování strategických cílů a směrování rozvoje v oblasti kybernetické bezpečnosti,
* definici rolí a odpovědností v rámci systému řízení informací,
* definici požadavků na podávání zpráv a kontrolu systému řízení bezpečnosti informací,
* kontrolu aktuálního stavu kybernetické bezpečnosti v rámci své působnosti a zjišťování, zda dochází k naplňování plánovaných cílů.

Dále se Výbor pro řízení kybernetické bezpečnosti podílí na:

* hodnocení účinnosti bezpečnostních opatření, jejich důsledků a vhodnosti pro dané prostředí, jakož i na identifikaci jim odpovídajících alternativ, vhodných pro organizaci,
* přípravě vzdělávacích a osvětových programů pro kybernetickou bezpečnost a posilování bezpečnostního povědomí v Organizace.

### Složení Výboru pro řízení kybernetické bezpečnosti

Členy Výboru jsou předseda, místopředseda a ostatní členové.

Předsedou Výboru je doplnit, do funkce je jmenován ředitelem Organizace. Místopředsedou Výboru je Manažer kybernetické bezpečnosti Organizace.

Ostatními členy Výboru jsou:

* doplnit
* další zástupci, o jejichž členství na návrh věcně příslušných náměstků Výbor rozhodne.

Každý člen může mít svého náhradníka, který ho zastupuje v případě nepřítomnosti v plném rozsahu práv a povinností.

Členové výboru a jejich náhradníci jsou do funkce jmenováni Předsedou výboru.

Výbor může na svá jednání přizvat stálé nebo dočasné hosty, zejména pokud je třeba doplnit odborné zázemí výboru. Hosté se nepodílejí na rozhodování Výboru.

## Manažer kybernetické bezpečnosti

Manažer kybernetické bezpečnosti zodpovídá 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 kybernetické bezpečnosti působí jako "kontaktní" osoba pro veškeré aspekty a otázky kybernetické bezpečnosti, která rovněž prosazuje a koordinuje úlohu systému řízení informační bezpečnosti v organizaci.

### Kvalifikační požadavky

Manažer kybernetické bezpečnosti je bezpečnostní role odpovědná za systém řízení bezpečnosti informací, přičemž výkonem této role může být pověřena pouze osoba, která splňuje kvalifikační předpoklady stanovené v příloze č. 6 VKB.

Současně musí mát osoba pověřená výkonem role Manažera kybernetické bezpečnosti odpovídající komunikační a manažerské dovednosti a schopnost týmové práce.

### Pravomoci a odpovědnosti role

Manažer kybernetické bezpečnosti je hlavním řídícím prvkem systému řízení bezpečnosti informací a je odpovědný za systém řízení bezpečnosti informací jako celek. Především odpovídá za realizaci všech nutných aktivit počínaje prevencí, přes průběžné testování, až po eliminaci následků a vyhodnocení kybernetických incidentů. Hlavní úlohou Manažera kybernetické bezpečnosti je naplňovat Bezpečnostní politiku informací schválenou Výborem.

Manažer kybernetické bezpečnosti odpovídá za vyřešení všech neshod a závad v rozsahu systému řízení bezpečnosti informací v organizaci. Hlavní úlohou Manažera kybernetické bezpečnosti je naplňovat Bezpečnostní politiku schválenou Výborem pro řízení kybernetické bezpečnosti. Působí také jako průvodce systémem kybernetické bezpečnosti pro ostatní členy bezpečnostního týmu, kterým na základě svých znalostí a zkušeností a přidělených pravomocí pomáhá vykonávat jejich role.

Vzhledem k nezbytnosti vysoké míry nezávislosti je nezbytná jak vysoká míra jednoznačně vymezených pravomocí, tak i vysoká míra osobní odpovědnosti za (ne)učiněná rozhodnutí. Role manažera kybernetické bezpečnosti není slučitelná s rolemi odpovědnými za provoz informačního a komunikačního systému a s dalšími provozními a řídícími rolemi.

**Klíčové činnosti:**

* odpovědnost za řízení systému řízení bezpečnosti informací,
* pravidelný reporting pro vrcholové vedení organizace,
* pravidelná komunikace s vrcholovým vedením organizace,
* předkládání Zpráv o hodnocení aktiv a rizik, Plánu zvládání rizik a Prohlášení o aplikovatelnosti Výboru pro řízení kybernetické bezpečnosti,
* poskytování pokynů pro zajištění bezpečnosti informací pří vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti ICT,
* komunikace s GovCERT / CSIRT,
* podílení se na procesu řízení rizik,
* koordinace řízení incidentů,
* vyhodnocování vhodnosti a účinnosti bezpečnostních opatření.

Manažer kybernetické bezpečnosti je i výkonným protějškem NÚKIB pro případy řešení kybernetických bezpečnostních událostí a incidentů.

Manažer kybernetické bezpečnosti bude rovněž seznámen se všemi projekty s dopadem na zpracování, přenos a ukládání informací, zavádění nových nebo změny existujících systémů a procedur s dopadem na bezpečnost informací, a to jak ve fázi jejich přípravy, tak aplikace. Cílem tohoto opatření je zajistit, že budou náležitě vzaty do úvahy veškeré aspekty kybernetické bezpečnosti ve fázích přípravy, realizace a implementace všech relevantních projektů.

## Architekt kybernetické bezpečnosti

Architekt kybernetické bezpečnosti je bezpečnostní role odpovědná za zajištění návrhu a implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému. Výkonem této role může být pověřena osoba, která splňuje kvalifikační předpoklady stanovené VKB.

### Hlavní úkoly Architekta KB

Architekt kybernetické bezpečnosti posuzuje všechny prvky tvořící informační aktiva organizace v jejich souvislostech a navrhuje možné cesty, případně způsoby dalšího rozvoje řízení informační bezpečnosti jako podklad pro rozhodování vedení organizace. Určuje a komunikuje klíčové podmínky, principy a modely, které popisují budoucí stav řízení kybernetické bezpečnosti organizace. Architekt kybernetické bezpečnosti se podílí na inicializaci změny, dává podněty, které vyplývají z koncepčně řízené bezpečnostní architektury, spolu inicializuje vznik strategických projektů, které naplňují požadavky zákona o kybernetické bezpečnosti a vyhlášky ke kybernetické bezpečnosti. Navrhuje rovněž základní bezpečnostní architektury informačních a komunikačních systémů, jejich jednotlivých komponent, vzájemných vazeb a dohlíží na soulad implementace základní architektury informačních a komunikačních systémů se systémem řízení kybernetické bezpečnosti.

### Kvalifikační požadavky

Architekt kybernetické bezpečnosti je bezpečnostní role odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému, přičemž výkonem této role může být pověřena pouze osoba, která splňuje kvalifikační předpoklady stanovené v příloze č. 6 VKB.

Současně musí mát osoba pověřená výkonem role Architekta kybernetické bezpečnosti odpovídající komunikační a manažerské dovednosti a schopnost týmové práce.

### Pravomoci a odpovědnosti role

Hlavní úlohou Architekta kybernetické bezpečnosti je na základě schválené bezpečnostní politiky organizace navrhnout a metodicky dozorovat implementace odpovídajících bezpečnostních opatření v organizaci a existující opatření průběžně analyzovat a s výsledky seznamovat Manažera kybernetické bezpečnosti a výbor.

Úkoly Architekta kybernetické bezpečnosti dále zahrnují popis stávajícího stavu KB, formulování požadovaného stavu KB a identifikaci kroků vedoucích k jeho dosažení. Dalšími úkoly jsou:

* definovat klíčové projekty, které vedou k naplnění bezpečnostní politiky a k cílovému stavu modelu architektury kybernetické bezpečnosti, dohlížet na jejich realizaci a vyhodnocení,
* analyzovat úrovně architektury kybernetické bezpečnosti, definovat pro ni metriky a identifikovat existující rizika a navrhovat strategie na zmírnění rizik,
* vytvářet plány implementace architektury kybernetické bezpečnosti organizace podle schválené bezpečnostní politiky, určovat části a milníky k dosažení očekávaného cílového stavu,
* navrhovat bezpečnostní opatření pro snižování rizik, připravovat pravidla a standardy pro oblast kybernetické bezpečnosti,
* vybírat a implementovat nástroje pro zajištění technických opatření kybernetické bezpečnosti,
* podílet se na pravidelném plánování v souladu se strategickými cíli organizace a na aktualizaci podnikové strategie kybernetické bezpečnosti a dalších částí,
* vytvářet a udržovat model podnikové architektury kybernetické bezpečnosti (procesní model, organizační struktura, aplikační architektura, technologie apod.),
* vyhodnocovat průběžně aktuální stav úrovně bezpečnosti informací podle stanovených metrik,
* průběžně analyzovat a vyhodnocovat informace v modelu podnikové architektury kybernetické bezpečnosti a udržovat ho ve vztahu k cílovému stavu.

## Auditor kybernetické bezpečnosti

Auditor kybernetické bezpečnosti musí být schopen efektivně provádět audity systému řízení kybernetické informační bezpečnosti organizace, zpracovávat požadovanou dokumentaci, včetně tvorby výstupních auditních zpráv a vyjádření k naplnění požadavků zákona o kybernetické bezpečnosti včetně vyhlášek na audity. Tato role přispívá k efektivnější ochraně systému řízení informační bezpečnosti u povinného subjektu.

Auditor kybernetické bezpečnosti:

* prověřuje fungování systémů řízení informační bezpečnosti organizace v souladu se zákonem o kybernetické bezpečnosti a jeho prováděcími předpisy, platnými mezinárodními ISO normami, případně se zásadami, standardy a směrnicemi organizace;
* kontroluje aktuálnost a dodržování platných zákonných i interními akty řízení stanovených procesních postupů, evidencí, školení a reportování identifikovaných kybernetických bezpečnostních událostí.

### Kvalifikační požadavky

Auditor kybernetické bezpečnosti je bezpečnostní role odpovědná za provádění auditu kybernetické bezpečnosti, přičemž výkonem této role může být pověřena pouze osoba, která splňuje kvalifikační předpoklady stanovené v příloze č. 6 VKB.

Současně musí mít osoba pověřená výkonem role Auditora kybernetické bezpečnosti odpovídající komunikační a manažerské dovednosti a schopnost týmové práce.

### Odpovědnosti a úkoly

Auditor kybernetické bezpečnosti odpovídá za formální i věcně správné a úplné provedení auditu kybernetické bezpečnosti v rozsahu organizace. Úkoly auditora kybernetické bezpečnosti zahrnují, mimo jiné:

* plánování činnosti auditu podle specifických podmínek auditované organizace,
* vedení dokumentace o průběhu auditu podle stanovených metodik,
* vyhodnocování shromážděných nálezů z auditu a jejich srovnávání s kritérii auditu,
* sdělování výsledků auditu a navrhování doporučení,
* zpracování závěrečných zpráv z auditu,
* kontrolování účinnosti přijatých opatření,
* re-auditní činnost.

Auditor kybernetické bezpečnosti musí být rovněž zapojen ve všech důležitých projektech s dopadem na zpracování a ukládání informací, zavádění nových systémů nebo změny existujících systémů a procedur s dopadem v oblasti bezpečnosti informací, aby bylo zajištěno, že v jejich rámci budou náležitě vzaty do úvahy veškeré aspekty informační bezpečnosti ve všech fázích jejich přípravy a aplikace.

Role Auditora kybernetické bezpečnosti může být outsourcována formou externí služby, v takovém případě je dodavatel zajišťující výkon role Auditora kybernetické bezpečnosti vázán jak řídící dokumentací systému řízení bezpečnosti informací Organizace, tak metodikami a pravidly provádění auditu kybernetické bezpečnosti a vnitřními předpisy upravujícími provádění řídící kontroly a interního auditu Organizace.

### Spolupráce a komunikace

Spolupráce se zaměstnanci a externími subjekty vyžaduje dobrou úroveň komunikačních technik a dovedností, protože významná část techniky auditů při sběru informací je prováděna formou osobních pohovorů. Auditor tak musí být schopen si informace nejen získat, ale také ověřit validitu těchto informací. Stejně tak osoba zastávající tuto roli musí být schopna prezentovat výsledky auditu v různých formách pro různé typy posluchačů, od nejvyššího vedení organizace až například pro pracovníky dotčených oddělení.

### Nezávislost Auditora KB

Role Auditora kybernetické bezpečnosti je neslučitelná s členstvím ve Výboru pro řízení kybernetické bezpečnosti, s rolí Manažera kybernetické bezpečnosti, Architekta kybernetické bezpečnosti a Garanta aktiva. Auditor kybernetické bezpečnosti vykonává svou roli nestranně. Musí být garantována nezávislost auditora vůči předmětu auditu.

## Garant aktiva

Garant aktiva je bezpečnostní role odpovědná za definici požadavků na rozvoj, použití a bezpečnost primárního nebo podpůrného aktiva. Je osobou zařazenou v systému řízení bezpečnosti informací organizace na nejnižším stupni řízení tak, že jeho pravomoci a odpovědnosti jsou vždy vztaženy na konkrétní aktivum, resp. třídu aktiv. Garant aktiva musí disponovat dobrou znalostí aktiva, jehož je garantem, a dobrou znalostí interních bezpečnostních politik a metodik. Garant aktiva spolupracuje s ostatními osobami zastávajícími bezpečnostní role.

Povinnosti týkající se aktiv, které jsou ZKB a VKB stanoveny povinným osobám uvedeným v § 3 písm. c) až g) ZKB, směřují k nastavení pravidel pro jejich řízení. Pravidla by měla garantovat zajištění důvěrnosti, integrity a dostupnosti aktiva, samozřejmě rozsahem a způsoby odpovídajícími jeho povaze.

### Obecné pravomoci a povinnosti garantů aktiv

Mezi obecné pravomoci a povinnosti garantů aktiv (dále jen „GA“) patří:

* definovat pravidla použití a ochrany aktiv,
* vymáhat dodržování těchto pravidel,
* navrhovat úpravy těchto pravidel.

Aktiva jsou velmi různorodé prvky a obsah pravidel použití a ochrany aktiv, stejně jako rosah používání a bezpečnosti, se bude měnit podle jejich podstaty (u technických systémů bude rozvoj znamenat např. aktualizaci systému za účelem zvýšení odolnosti vůči novým bezpečnostním hrozbám, zatímco u osob půjde např. o jejich poučení o nových bezpečnostních hrozbách, atp.). Pravomoci a povinnosti garanta aktiva vždy směřují k zajištění a udržení potřebné úrovně bezpečnosti daného aktiva.

Obecně pro garanty aktiv platí, že nedisponují-li k výkonu svých funkcí patřičnými kompetencemi nebo zdroji, vznáší podněty v rámci organizační struktury organizace, případně informují Manažera kybernetické bezpečnosti.

Povinné osoby především musí v organizaci nastavit systém řízení bezpečnosti informací, v rámci kterého vytvoří i sadu pravidel pro řízení aktiv, která přiřadí jednotlivým GA. Pravomoci a povinnosti GA jsou odvozeny až od těchto pravidel, která budou vycházet z konkrétní faktické situace organizace.

### Garant primárního aktiva

Primární aktivum je dle § 2 písm. g) VKB informace nebo služba, kterou dotčený systém zpracovává nebo poskytuje.

Garant primárního aktiva (dále jen „GpA“)

* je fyzická osoba pověřená k zajištění rozvoje, použití a bezpečnosti primárního aktiva (zajištění důvěrnosti, dostupnosti a integrity aktiva).
* je vlastníkem aktiva z pohledu nikoliv majetkového, ale odpovědnostního, jedná se o osobu, která je zodpovědná za jeho chod po obsahové stránce (např. o správce aplikace).

Úkolem GpA je nadefinovat požadavky na zabezpečení primárního aktiva a to jak zabezpečení důvěrnosti, dostupnosti, tak i integrity dat. Ve většině případů je toto řešeno definováním požadavků, které následně řeší garanti podpůrných aktiv.

### Garant podpůrného aktiva

Podpůrnými aktivy jsou podle § 2 písm. f) a k) VKB technické vybavení, komunikační prostředky dotčeného systému a jeho programové vybavení, objekty, ve kterých je tento systém umístěn, dále zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti aktiva.

Garant podpůrného (technického) aktiva (dále jen „GtA“)

* je fyzická osoba pověřená k zajištění rozvoje, použití a bezpečnosti technického aktiva, hodnotí se zajištění vazeb na primární aktiva.
* je nejčastěji administrátor, technický správce serverů, sítě apod. = osoba odpovědná za chod zařízení s dodržením nastavených parametrů poskytovaných služeb.

## RACI matice zákonných bezpečnostních rolí

Matice odpovědnosti RACI je jednou z metod používaných pro přiřazení a zobrazení odpovědností jednotlivých zákonných kybernetických rolí. RACI je akronym z počátečních písmen slov:

**R** Responsible – kdo je odpovědný za vykonání svěřeného úkolu

**A** Accountable (někdy též Approver) – kdo je odpovědný za celý úkol, je odpovědný za to, co je vykonáno

**C** Consulted – kdo může poskytnout cennou radu či konzultaci k úkolu

**I** Informed – kdo má být informován o průběhu úkolu či rozhodnutích v úkolu

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Výbor KB** | **Manažer KB** | **Architekt KB** | **Auditor KB** | **Garant aktiva** |
| Celkové řízení a rozvoj KB | A, R | C, I | C, I | C, I | C, I |
| Audit KB | A, I, C | C, I | C, I | R | C, I |
| Systém řízení bezpečnosti informací | A, I, C | R | C, I | C | C, I |
| Návrh bezpečnostních opatření | I, C | A, C, I | R | C | C, I |
| Implementace bezpečnostních opatření | I, C | A, C, I | R | C | C, I |
| Zajištění rozvoje, použití a bezpečnosti aktiva | I, C | A, C, I | C, I | C | R |

Tabulka 1 – Matice rolí

Detailní RACI matice pro výkon jednotlivých procesů či plnění konkrétních úkolů jsou součástí příslušných politik a metodik systému řízení bezpečnosti informací Organizace.

## Vyškolení rolí kybernetické bezpečnosti

Všechny osoby, které se budou podílet na zajišťování rolí souvisejících s řízením kybernetické bezpečnosti, budou odpovídajícím způsobem vyškoleny a průběžně vzdělávány. Odpovědnost za zpracování, průběžnou aktualizaci a sledování naplňování plánu vzdělávání pro všechny role má Manažer kybernetické bezpečnosti.

Oblast personálního rozvoje a vzdělávání je uvedena ve schváleném dokumentu „Plán rozvoje bezpečnostního povědomí“.

# Procesy a zásady řízení bezpečnosti informací

## Klasifikace a řízení informačních aktiv

Účelem procesu klasifikace a řízení informačních aktiv je udržovat přiměřenou ochranu informačních aktiv.

Při klasifikaci a řízení informačních aktiv jsou uplatňovány následující bezpečnostní zásady:

1. v rámci Organizace je zavedena a udržována evidence informační infrastruktury a systémů včetně informace o jejich správcích
2. jednotliví správci IS/ICT vedou evidenci důležitých informačních aktiv, u nichž je určen garant a jednoznačně stanovena odpovědnost za dodržování povinností při jejich zpracování, shromažďování a uchovávání v souladu s platnými právními a organizačními předpisy,
3. informační aktiva Organizace jsou klasifikována tak, aby byla stanovena jejich potřebnost, důležitost a stupeň ochrany při manipulaci s nimi,
4. klasifikaci stanoví garanti aktiv nebo vlastníci procesů, kteří odpovídají za periodické přezkoumávání této klasifikace a její aktualizaci,
5. klasifikace určuje způsob zacházení s informacemi s ohledem na jejich ochranu.

Problematika identifikace aktiv a jejich klasifikace je upravena v samostatné metodice.

## Kritéria hodnocení rizik

Bezpečnostní opatření jsou vybrána na základě prováděného hodnocení rizik a požadavků zákonných norem. Hodnocení rizik je prováděno na základě následujících kritérií:

1. stanovení hodnot informačních aktiv Organizace z hlediska požadavků na jejich dostupnost, důvěrnost a integritu,
2. určení možných dopadů identifikovaných hrozeb, reálné pravděpodobnosti jejich uskutečnění a určení úrovně rizik pro aktiva,
3. určení akceptovatelné úrovně rizika pro informační aktiva Organizace.

Problematika analýzy a řízení rizik je upravena v samostatné metodice.

## Řízení lidských zdrojů

Účelem procesu řízení bezpečnosti lidských zdrojů je snížení rizika lidské chyby, krádeže, podvodu nebo zneužití prostředků Organizace. Bezpečnostní cíle v oblasti řízení lidských zdrojů zahrnují zajištění:

1. vhodných postupů v rámci přijímacího řízení
2. povědomí zaměstnanců o bezpečnosti informací
3. vhodných postupů v rámci změny pracovní pozice
4. vhodných postupů v rámci ukončení pracovního poměru

Pro oblast personální bezpečnosti jsou v rámci Organizace stanoveny následující bezpečnostní zásady:

1. posuzování uchazečů o zaměstnání z hlediska personální bezpečnosti je součástí výkonu personálních činností dle Pracovního řádu a v souladu s obsahem pracovněprávních dokumentů v personálních šablonách,
2. zaměstnanci učiní písemné prohlášení o mlčenlivosti ve smyslu zákonem uložené povinnosti,
3. zaměstnanci Organizace jsou povinni zachovávat mlčenlivost o skutečnostech, se kterými se seznámili při plnění svých pracovních úkolů nebo v přímé souvislosti s nimi a tato povinnost trvá i po skončení pracovního vztahu, pokud zvláštní právní předpis nestanoví jinak,
4. seznámení zaměstnanců s Bezpečnostní politikou je součástí vstupního školení a dalších periodických školení,
5. zaměstnanci musí znát postupy hlášení bezpečnostních incidentů,
6. nedodržení bezpečnostních zásad může být kvalifikováno jako porušení povinností zaměstnance příp. porušení pracovní kázně s příslušnými důsledky pro zaměstnance, ve smyslu zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, pokud se nejedná o přestupek podle § 44 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů nebo trestný čin podle § 180 zákona č. 40/2009Sb., trestní zákoník, ve znění pozdějších předpisů,
7. šetření závažných bezpečnostních incidentů zajišťuje Manažer kybernetické bezpečnosti včetně zpracování protokolů o bezpečnostních incidentech, jejich evidence a předložení návrhů Organizace k zajištění bezpečnosti.

## Řízení fyzické bezpečnosti

Účelem fyzické bezpečnosti a bezpečnosti prostředí je předcházet neoprávněnému a / nebo neautorizovanému přístupu k informacím, poškození a narušení informací. Bezpečnostním cílem je zajištění fyzické ochrany informací a prostředí, ve kterém se informace nacházejí. Cíle je dosahováno prostřednictvím následujících opatření:

1. vymezením a využíváním zabezpečených oblastí, zahrnujících kontrolu vstupu a upřesněním způsobu práce osob v těchto oblastech, zabezpečením kanceláří, místností a zařízení, ochranou proti hrozbám působícím z vnějšího prostředí, zejména tam, kde se informace nacházejí, zpracovávají a uchovávají,
2. zabezpečením zařízení proti odcizení a zničení, poškození, zahrnujícím bezpečné umístění zařízení, zajištěním podpůrných služeb pro provoz zařízení (dodávky energie, klimatizace atd.), zabezpečením kabeláže a zajištěním pravidelné a bezpečné údržby zařízení,
3. zajištěním bezpečnosti informací mimo objekty Organizace.

Pro oblast personální bezpečnosti jsou v rámci Organizace stanoveny následující bezpečnostní zásady:

1. stanovení režimu vstupu a výstupu osob včetně zajištění zabezpečených oblastí a definování fyzického bezpečnostního perimetru; pravidla jsou stanovena samostatnou politikou a společnou dokumentací Organizace,
2. zajištění požární bezpečnosti podle zákonů a jiných právních předpisů; pravidla jsou upravena zvláštní vnitřní organizační politikou,
3. vstup do budov oprávněným orgánům ke zdolání požáru nebo k provedení jiných záchranných prací dle rozhodnutí velitele zásahu stanovuje dokumentace zdolávání požáru a navazující dokumentace požární ochrany,
4. kontrola dodržování zásad čistého stolu a čisté obrazovky spadá do kompetence vedoucích zaměstnanců.

## Řízení preventivních a nápravných opatření

Pro oblast řízení preventivních a nápravných opatření jsou stanoveny bezpečnostní zásady, které jsou zapracovány do bezpečnostní dokumentace jednotlivých aktiv. Tyto zásady zohlední při své činnosti jednotliví garanti aktiv.

## Řízení bezpečnosti komunikací a provozu

Účelem procesu řízení bezpečnosti komunikací a provozu je zajistit správný a bezpečný provoz prostředků pro zpracování informací, minimalizovat riziko selhání systému, chránit integritu a dostupnost programů, dat a informačních systémů, chránit důvěrnost informací a zajistit ochranu počítačových sítí.

Pro oblast řízení bezpečnosti komunikací a provozu jsou v rámci Organizace stanoveny následující bezpečnostní zásady:

1. je využívána ochrana proti škodlivým a automaticky spouštěným programům,
2. je prováděno zálohování, které zajistí obnovu dat a systémů ve vazbě na zachování základních funkcí Organizace,
3. jsou zpracovány postupy obnovy po selhání nebo výpadku systému pro zpracování a uchování informací,
4. je prováděno zajišťování bezpečnosti komunikační infrastruktury,
5. je zajištěna dostupnost informací a služeb,
6. je zajištěna důvěrnost informací při jejich přenosu pomocí kryptografické ochrany,
7. je zajištěna ochrana před neautorizovanými zásahy dodržováním principu oddělení povinností a odpovědností při přidělování uživatelských práv,
8. je prováděno monitorování provozu a zaznamenávání událostí,
9. jsou přijata opatření pro zajištění bezpečnosti elektronické pošty,
10. je vymáháno dodržování bezpečnosti při zacházení s paměťovými médii.

## Řízení přístupu

Účelem procesu řízení přístupu k informacím a prostředkům informačních systémů Organizace je zajistit, aby k nim měli přístup pouze oprávnění uživatelé. Pro přístup k těmto informacím a prostředkům jsou stanovena pravidla, která určují postupy pro autorizaci, zřizování, změny a odebírání přístupových práv, systém správy přístupu zajišťuje definovaný postup přidělování, změny a odebírání přístupu, správu hesel a kontrolu přístupových práv. Jsou nastavena samostatná pravidla pro řízení přístupových práv mobilních zařízení.

## Vývoj a údržba systémů

Účelem řízení bezpečnosti v oblasti vývoje a údržby systémů je prosadit bezpečnost informací do celého životního cyklu provozovaných informačních systémů od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu. Implementace a změny informačních systémů Organizace jsou spojeny se stanovením vhodných bezpečnostních požadavků.

Bezpečnostním cílem v oblasti vývoje a údržby systémů je zajištění ochrany prostřednictvím opatření v následujících oblastech:

1. analýza a specifikace bezpečnostních požadavků – určení bezpečnostních požadavků v klíčových fázích životního cyklu informačního systému zajistí, aby bezpečnost byla nedílnou součástí informačních systémů;
2. zajištění přesnosti a spolehlivosti zpracování dat v aplikacích a kryptografická opatření – validace a kontrola dat má spolu s kryptografickými opatřeními za cíl předcházet ztrátě, neoprávněné modifikaci nebo zneužití dat v aplikacích;
3. bezpečnost systémových souborů a procesu vývoje a podpory – je nutné zabezpečit systémové soubory a zdrojový kód a kontrolovat postupy vývoje a podpory, včetně formalizovaného postupu řízení změn;
4. správa zranitelností – je nutné vhodnými opatřeními omezit rizika vyplývající ze zneužití publikovaných zranitelností.

Vývoj a údržbu informačních systémů v rozsahu infrastruktury Organizace a uživatelsky vyvinutých aplikací podle stanovené působnosti zajišťují garanti jednotlivých aktiv ve spolupráci s dodavateli včetně zajišťování implementace Bezpečnostní politiky v oblasti procesů IT.

## Řízení dodavatelů

Požadavky bezpečnosti informací na snížení rizik spojených s přístupem dodavatelů k aktivům Organizace musí být odsouhlaseny s dodavateli a dokumentovány.

Bezpečnostní cíle stanovené pro oblast řízení dodavatelů zahrnují:

1. zajištění ochrany aktiv Organizace, ke kterým mají dodavatelé přístup,
2. udržování dohodnuté úrovně bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami.

Pro oblast řízení dodavatelů jsou v rámci Organizace stanoveny následující bezpečnostní zásady:

1. každý dodavatel, který může přistupovat k informacím Organizace, zpracovávat je, ukládat, komunikovat nebo je zajišťovat prvky IT infrastruktury, je zavázán k dodržování všech relevantních požadavků bezpečnosti informací,
2. dohody s dodavateli zahrnují požadavky na řízení rizik bezpečnosti informací spojených s dodavatelským řetězcem služeb a produktů informačních a komunikačních technologií,
3. Organizace pravidelně monitoruje, přezkoumává a audituje dodávky služeb dodavatelů,
4. změny v poskytování služeb dodavateli, včetně změn v udržování a zlepšování existujících politik, postupů a opatření bezpečnosti informací, jsou řízeny s ohledem na kritičnost informací, systémů a procesů Organizace, které jsou součástí těchto změn, a s ohledem na opakované posouzení rizik.

## Řízení kontinuity činností

Záměrem Organizace je zajistit připravenost k řešení krizových situací a zachování základních funkcí v definovaném rozsahu fungování.

Bezpečnostním cílem je zajištění přípravy, proškolení a připravenosti určených zaměstnanců Organizace po odborné stránce k výkonu činností spojených s řešením krizových situací, ochranou zdraví a života zaměstnanců a ochranou majetku.

Pro oblast řízení kontinuity činností jsou v rámci Organizace stanoveny následující bezpečnostní zásady:

1. rozhodnutí o zablokování komunikace konkrétních komponent nebo celého IS/ICT Organizace, případně jiném opatření omezujícím služby IS/ICT, zavedeném na základě detekované bezpečnostní události, spadá do kompetence Manažera kybernetické bezpečnosti, který je oprávněn tuto kompetenci v definovaných případech delegovat na garanty odpovídajících aktiv,
2. realizace přechodu na krizové řízení spadá do kompetence Manažera kybernetické bezpečnosti Organizace
3. realizace opatření k zachování základních funkcí spadá do kompetence Manažera kybernetické bezpečnosti Organizace.

## Soulad s požadavky na ochranu informací

Pro zabezpečení informací Organizace jsou jednoznačně definovány a zdokumentovány všechny relevantní zákonné a smluvní požadavky. V rámci Organizace je veden přehled platných právních norem a předpisů vztahujících se k problematice bezpečnosti informací.

Pro oblast souladu s požadavky jsou v rámci Organizace stanoveny následující bezpečnostní zásady:

1. Organizace dodržuje ustanovení o autorském právu a podmínky licenčních ujednání dodavatelů programového vybavení,
2. Organizace provádí posouzení shody Bezpečnostní politiky informací Organizace a navazujících předpisů se skutečným stavem bezpečnosti informací a k zajištění souladu informačního systému Organizace s příslušnými technickými normami je prováděno posouzení shody,
3. Organizace přijímá a provádí opatření k zajištění ochrany osobních údajů a citlivých údajů v souladu s příslušnými právními předpisy.

## Odpovědnosti pro bezpečnost informací

Pro oblast bezpečnosti informací jsou stanoveny obecné a specifické odpovědnosti takto:

1. obecné povinnosti pro oblast bezpečnosti informací vyplývají pro zaměstnance Organizace ze směrnic EU, zákonů a jiných právních předpisů ČR,
2. specifické povinnosti pro oblast bezpečnosti informací vyplývají pro zaměstnance Organizace zejména z vnitřních organizačních směrnic, povinností uložených nadřízenými vedoucími zaměstnanci a dle pracovního zařazení,
3. Bezpečnostní politiku informací jsou povinni dodržovat všichni zaměstnanci Organizace; její plnění kontrolují vedoucí zaměstnanci v rozsahu stanovené působnosti a odpovědnosti,
4. kontrolní činnost v oblasti bezpečnosti informací metodicky usměrňuje Manažer kybernetické bezpečnosti.

## Přezkoumávání a audity

Organizace pravidelně realizuje nezávislé audity stavu informační bezpečnosti a plnění legislativních požadavků v této oblasti.

Audity jsou zaměřeny na posouzení souladu dosaženého stavu bezpečnosti informací s požadavky ZKB a jeho prováděcích předpisů a s požadavky norem řady ISO/IEC 27000 na řízení systému bezpečnosti informací jakož i dalších předpisů a norem relevantních pro řízení bezpečnosti informací v Organizaci. Cílem provádění auditů je nezávislé prověření aktuálního stavu bezpečnosti informací.

Pro oblast přezkoumání a auditu kybernetické bezpečnosti jsou v rámci Organizace stanoveny následující bezpečnostní zásady:

1. přístup Organizace k řízení a implementaci bezpečnosti informací (tj. cílů opatření, jednotlivých opatření, politik, procesů a postupů bezpečnosti informací) je nezávisle přezkoumáván v plánovaných intervalech, nebo když nastane významná změna,
2. vedoucí zaměstnanci musí pravidelně přezkoumávat shodu zpracování informací a postupů v rozsahu jejich odpovědnosti s odpovídajícími bezpečnostními politikami, normami a dalšími požadavky na bezpečnost,
3. informační systémy musí být pravidelně přezkoumávány, zda jsou v souladu s politikami a normami bezpečnosti informací Organizace.

Metodiku auditu řízení kybernetické bezpečnosti upravuje samostatná závazná metodika Organizace.

# Struktura bezpečnostní dokumentace

V rámci řízení kybernetické bezpečnosti Organizace udržuje systém dokumentace upravující jednotlivé aspekty kybernetické bezpečnosti Organizace. Tento systém má několik úrovní dokumentů.

## Obecná bezpečnostní dokumentace

Organizace zpracovala a udržuje strategické dokumenty definující hlavní principy a parametry kybernetické bezpečnosti . Tyto dokumenty jsou pro Organizaci závazné a není možné se od nich odchýlit.

Jedná se o následující dokumenty:

* Bezpečnostní politika informací
* Strategie kybernetické bezpečnosti

## Bezpečnostní dokumentace

Bezpečnostní dokumentace Organizace obsahuje:

* [vybrat, co bude skutečně zpacováno]
* Systém řízení bezpečnosti informací
* Politika organizační bezpečnosti
* Politika řízení vztahů s dodavateli
* Politika klasifikace aktiv
* Politika bezpečnosti lidských zdrojů
* Politika řízení provozu a komunikací
* Politika řízení přístupu
* Politika bezpečného chování uživatelů
* Politika zálohování a obnovy
* Politika poskytování a nabývání licencí programového vybavení a informací
* Politika ochrany osobních údajů
* Politika ochrany před škodlivým kódem
* Politika nasazení a používání nástrojů pro detekci kybernetických bezpečnostních událostí
* Politika používání kryptografické ochrany
* Politika bezpečného předávání a výměny informací,
* Politika řízení technických zranitelností,
* Politika bezpečného používání mobilních zařízení,
* Politika dlouhodobého ukládání a archivace informací,
* Politika fyzické bezpečnosti,
* Politika bezpečnosti komunikační sítě,
* Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

***Doporučení Ministerstva zdravotnictví****: Jednotlivé výše uvedené politiky nemusí být zpracovány vždy jako samostatný dokument, nicméně řídící dokumentace kybernetické bezpečnosti musí pokrývat všechny určené oblasti definované výše uvedenými seznamy.*

Současně Organizace vede provozní dokumentaci v následujícím rozsahu:

* [vybrat, co bude skutečně vedeno]
* zprávy z auditu kybernetické bezpečnosti,
* zprávy z přezkoumání systému řízení bezpečnosti informací,
* metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik,
* zprávu o hodnocení rizik,
* prohlášení o aplikovatelnosti,
* plán zvládání rizik,
* plán rozvoje bezpečnostního povědomí,
* zvládání kybernetických bezpečnostních incidentů,
* strategii řízení kontinuity činností,
* přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků.

# Závěrečná ustanovení

Tato politika nabývá účinnosti dnem bude doplněno.

1. [↑](#footnote-ref-2)