|  |
| --- |
| *1.1.2020_Logolink barevné provedení - eso II*  **VZOR SMĚRNICE**  **Politika organizačních A Technických opatření kybernetické bezpečnosti**  **pro obec s rozšířenou působností**  Dokument byl zpracován v rámci realizace projektu  „Efektivní řízení rozvoje obcí jako základní předpoklad efektivnosti výkonu veřejné správy  a poskytování veřejných služeb z úrovně obcí“,  registrační číslo projektu: č.CZ.03.4.74/0.0/0.0/15\_019/0010159 |
| |  | | --- | |  | |  | | **VNITŘNÍ ORGANIZAČNÍ PŘEDPIS**  **XXXXXX** | |  | | **směrnice č. X/XXXX**  **Politika organizačních A Technických opatření kybernetické bezpečnosti**  **XXXXXX** | |
|  |

Revize dokumentu

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Poř.  číslo: | Datum: | Výsledek revize: | Revizi provedl: | Výsledek revize schválil/dne: |
| 1. | XX.XX.XXXX | Schváleno |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Platnost dokumentu

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ověřil: |  | Dne: | XX.XX.XXXX | Podpis: |
| Schválil: |  | Dne: | XX.XX.XXXX | Podpis: |
| Účinnost od: | XX.XX.XXXX | | | |
| Vydal: | XXXXXXXXX | | | |
| Počet stran: | 76 | | | |
| Počet příloh: | 0 | | | |
| Vydání: | první – verze 1.0 | | | |
| Dokument: | **INTERNÍ** | | | |

Obsah

[Úvodní ustanovení 10](#_Toc136334743)

[1. Předmět úpravy 10](#_Toc136334744)

[2. Rozsah platnosti 10](#_Toc136334745)

[3. Pojmy a zkratky 10](#_Toc136334746)

[4. Odpovědnosti a pravomoci 13](#_Toc136334747)

[5. Související dokumenty 13](#_Toc136334748)

[Směrnice č. X/XXXX Politika bezpečnosti informací. 13](#_Toc136334749)

[6. Odpovědnosti a pravomoci 13](#_Toc136334750)

[7. Souhrn politik organizačních a technických opatření kybernetické a informační bezpečnosti 14](#_Toc136334751)

[7.1. Politika systému řízení informační bezpečnosti 14](#_Toc136334752)

[7.2. Politika organizační bezpečnosti 14](#_Toc136334753)

[7.3. Politika řízení aktiv 14](#_Toc136334754)

[7.4. Politika řízení dodavatelů 15](#_Toc136334755)

[7.5. Politika bezpečnosti lidských zdrojů 16](#_Toc136334756)

[7.6. Politika řízení provozu a komunikací 16](#_Toc136334757)

[7.7. Politika řízení změn 17](#_Toc136334758)

[7.8. Politika řízení přístupu 17](#_Toc136334759)

[7.9. Politika bezpečného chování uživatelů 17](#_Toc136334760)

[7.10. Politika zálohování a obnovy a dlouhodobého ukládání 18](#_Toc136334761)

[7.11. Politika bezpečného předávání a výměny informací 18](#_Toc136334762)

[7.12. Politika řízení technických zranitelností 19](#_Toc136334763)

[7.13. Politika řízení kontinuity činností 19](#_Toc136334764)

[definuje v případě přerušení činností: 19](#_Toc136334765)

[7.14. Politika zvládání kybernetických bezpečnostních incidentů 20](#_Toc136334766)

[7.15. Politika akvizice, vývoje a údržby 20](#_Toc136334767)

[7.16. Politika fyzické bezpečnosti 20](#_Toc136334768)

[7.17. Politika bezpečnosti komunikační sítě 21](#_Toc136334769)

[7.18. Politika ochrany před škodlivým kódem 21](#_Toc136334770)

[7.19. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí 21](#_Toc136334771)

[7.20. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí 22](#_Toc136334772)

[Příloha č.1 23](#_Toc136334773)

[1. Politika systému řízení bezpečnosti informací 23](#_Toc136334774)

[1.1. Předmět 23](#_Toc136334775)

[1.2. Cíle, principy a potřeby řízení bezpečnosti informací 23](#_Toc136334776)

[1.3. Rozsah a hranice systému řízení bezpečnosti informací 24](#_Toc136334777)

[1.4. Pravidla a postupy pro řízení dokumentace 24](#_Toc136334778)

[1.5. Pravidla a postupy řízení provozu a zdrojů systému řízení bezpečnosti informací 26](#_Toc136334779)

[1.6. Pravidla a postupy pro provádění auditů kybernetické bezpečnosti 27](#_Toc136334780)

[1.7. Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací 27](#_Toc136334781)

[1.8. Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací 27](#_Toc136334782)

[2. Politika organizační bezpečnosti 28](#_Toc136334783)

[2.1. Předmět 28](#_Toc136334784)

[2.2. Rozsah působnosti 28](#_Toc136334785)

[2.3. Určení bezpečnostních rolí 28](#_Toc136334786)

[2.4. Výbor pro řízení kybernetické bezpečnosti, jeho práva a povinnosti 29](#_Toc136334787)

[2.5. Manažer kybernetické bezpečnosti, jeho práva a povinnosti 30](#_Toc136334788)

[2.6. Architekt kybernetické bezpečnosti, jeho práva a povinnosti 30](#_Toc136334789)

[2.7. Auditor kybernetické bezpečnosti, jeho práva a povinnosti 31](#_Toc136334790)

[2.8. Garant primárního aktiva, jeho práva a povinnosti 31](#_Toc136334791)

[2.9. Garant podpůrného aktiva, jeho práva a povinnosti 32](#_Toc136334792)

[2.10. Bezpečnostní správce, jeho práva a povinnosti 32](#_Toc136334793)

[2.11. Administrátor informačních systémů a technologií, jeho práva a povinnosti 32](#_Toc136334794)

[2.12. Bezpečnostní procesy pro bezpečnostní role kybernetické bezpečnosti 33](#_Toc136334795)

[2.13. Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí 35](#_Toc136334796)

[3. Politika řízení aktiv 35](#_Toc136334797)

[3.1. Předmět 35](#_Toc136334798)

[3.2. Rozdělení aktiv 35](#_Toc136334799)

[3.3. Garant aktiva 36](#_Toc136334800)

[3.4. Identifikace primárních aktiv 36](#_Toc136334801)

[3.5. Hodnocení primárních aktiv 37](#_Toc136334802)

[3.6. Evidence primárních aktiv 38](#_Toc136334803)

[3.7. Identifikace, hodnocení a evidence podpůrných aktiv 39](#_Toc136334804)

[3.8. Pravidla ochrany jednotlivých úrovní aktiv 39](#_Toc136334805)

[3.9. Způsoby spolehlivého mazání nebo ničení technických nosičů dat a jejich kopií 40](#_Toc136334806)

[4. Politika řízení dodavatelů 41](#_Toc136334807)

[4.1. Předmět 41](#_Toc136334808)

[4.2. Pravidla a principy pro výběr dodavatelů 41](#_Toc136334809)

[4.3. Pravidla pro hodnocení rizik dodavatelů 41](#_Toc136334810)

[4.4. Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti. 42](#_Toc136334811)

[4.5. Pravidla pro provádění kontroly zavedení bezpečnostních opatření 42](#_Toc136334812)

[4.6. Pravidla pro informování významného dodavatele 43](#_Toc136334813)

[4.7. Pravidla pro hodnocení dodavatelů 43](#_Toc136334814)

[5. Politika bezpečnosti lidských zdrojů 43](#_Toc136334815)

[5.1. Předmět 43](#_Toc136334816)

[5.2. Organizace řízení bezpečnosti lidských zdrojů 44](#_Toc136334817)

[5.3. Ukončení a změna pracovního poměru 45](#_Toc136334818)

[6. Politika řízení provozu a komunikací 46](#_Toc136334819)

[6.1. Předmět 46](#_Toc136334820)

[6.2. Pravomoci a odpovědnosti spojené s bezpečným provozem 46](#_Toc136334821)

[6.3. Postupy bezpečného provozu 46](#_Toc136334822)

[6.4. Řízení změn 46](#_Toc136334823)

[6.5. Řízení kapacit 47](#_Toc136334824)

[6.6. Oddělení prostředí vývoje, testování a provozu 47](#_Toc136334825)

[6.7. Zaznamenávání událostí 47](#_Toc136334826)

[6.8. Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů 48](#_Toc136334827)

[7. Politika řízení změn 48](#_Toc136334828)

[7.1. Předmět 48](#_Toc136334829)

[7.2. Způsob a principy řízení změn v procesech a informačních a komunikačních systémech 48](#_Toc136334830)

[7.3. Přezkoumávání dopadů změn 49](#_Toc136334831)

[7.4. Způsob vedení evidence a testování změn 49](#_Toc136334832)

[8. Politika řízení přístupu 50](#_Toc136334833)

[8.1. Předmět 50](#_Toc136334834)

[8.2. Pravidla a požadavky na řízení přístupu 50](#_Toc136334835)

[8.3. Princip minimálních oprávnění a potřeby znát (need to know) 51](#_Toc136334836)

[8.4. Minimální požadavky na systém řízení přístupu 51](#_Toc136334837)

[8.5. Životní cyklus řízení přístupu 51](#_Toc136334838)

[8.6. Řízení privilegovaných oprávnění 52](#_Toc136334839)

[8.7. Řízení přístupu pro mimořádné situace 52](#_Toc136334840)

[8.8. Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách 52](#_Toc136334841)

[9. Politika bezpečného chování uživatelů 53](#_Toc136334842)

[9.1. Předmět 53](#_Toc136334843)

[9.2. Pravidla pro bezpečné nakládání s aktivy 53](#_Toc136334844)

[9.3. Bezpečné použití přístupového hesla 53](#_Toc136334845)

[9.4. Bezpečné použití elektronické pošty a přístupu na internet 54](#_Toc136334846)

[9.5. Bezpečný vzdálený přístup 54](#_Toc136334847)

[9.6. Bezpečné chování na sociálních sítích 54](#_Toc136334848)

[9.7. Sdílení informací s vysokou úrovní důvěrnosti 55](#_Toc136334849)

[9.8. Bezpečnost ve vztahu k mobilním zařízením 55](#_Toc136334850)

[10. Politika zálohování a obnovy a dlouhodobého ukládání 56](#_Toc136334851)

[10.1. Předmět 56](#_Toc136334852)

[10.2. Požadavky na zálohování a obnovu 56](#_Toc136334853)

[10.3. Pravidla a postupy zálohování 56](#_Toc136334854)

[10.4. Pravidla a postupy dlouhodobého ukládání 56](#_Toc136334855)

[10.5. Pravidla bezpečného zálohování a dlouhodobého ukládání informací 57](#_Toc136334856)

[10.6. Pravidla a postupy obnovy 57](#_Toc136334857)

[10.7. Pravidla a postupy testování zálohování a obnovy 57](#_Toc136334858)

[10.8. V případě zjištění chyb při testu je nutno přijmout opatření k nápravě. 57](#_Toc136334859)

[11. Politika bezpečného předávání a výměny informací 58](#_Toc136334860)

[11.1. Předmět 58](#_Toc136334861)

[11.2. Pravidla a postupy pro ochranu předávaných informací 58](#_Toc136334862)

[11.3. Pravidla pro využívání kryptografické ochrany 59](#_Toc136334863)

[12. Politika řízení technických zranitelností 59](#_Toc136334864)

[12.1. Předmět 59](#_Toc136334865)

[12.2. Technické zranitelnosti ICT produktů 59](#_Toc136334866)

[12.3. Pravidla pro omezení instalace programového vybavení 59](#_Toc136334867)

[12.4. Pravidla a postupy vyhledávání opravných programových balíčků 60](#_Toc136334868)

[12.5. Pravidla a postupy testování oprav programového vybavení 60](#_Toc136334869)

[12.6. Pravidla a postupy nasazení oprav programového vybavení 60](#_Toc136334870)

[13. Politika řízení kontinuity činností 61](#_Toc136334871)

[13.1. Předmět 61](#_Toc136334872)

[13.2. Cíle řízení kontinuity činností 61](#_Toc136334873)

[13.3. Naplnění cílů kontinuity činností 61](#_Toc136334874)

[13.4. Způsoby hodnocení dopadů bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik 62](#_Toc136334875)

[13.5. Určení a obsah potřebných plánů kontinuity činností a havarijních plánů 62](#_Toc136334876)

[14. Politika zvládání kybernetických bezpečnostních incidentů 62](#_Toc136334877)

[14.1. Předmět 62](#_Toc136334878)

[14.2. Definování kategorií kybernetického bezpečnostního incidentu 62](#_Toc136334879)

[14.3. Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů 63](#_Toc136334880)

[14.4. Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů 63](#_Toc136334881)

[14.5. Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti 63](#_Toc136334882)

[14.6. Evidence incidentů 63](#_Toc136334883)

[15. Politika akvizice, vývoje a údržby 64](#_Toc136334884)

[15.1. Předmět 64](#_Toc136334885)

[15.2. Bezpečnostní požadavky pro akvizici, vývoj a údržbu 64](#_Toc136334886)

[15.3. Řízení zranitelností 65](#_Toc136334887)

[15.4. Poskytování a nabývání licencí programového vybavení a informací 66](#_Toc136334888)

[15.5. Způsoby ochrany elektronické výměny informací 66](#_Toc136334889)

[16. Politika fyzické bezpečnosti 67](#_Toc136334890)

[16.1. Předmět 67](#_Toc136334891)

[16.2. Pravidla pro ochranu objektů 67](#_Toc136334892)

[16.3. Pravidla pro kontrolu vstupu osob 68](#_Toc136334893)

[16.4. Pravidla pro ochranu zařízení 68](#_Toc136334894)

[16.5. Detekce narušení fyzické bezpečnosti 68](#_Toc136334895)

[17. Politika bezpečnosti komunikační sítě 68](#_Toc136334896)

[17.1. Předmět 68](#_Toc136334897)

[17.2. Pravidla a postupy pro zajištění bezpečnosti sítě 68](#_Toc136334898)

[17.3. Určení práv a povinností za bezpečný provoz sítě 68](#_Toc136334899)

[17.4. Pravidla a postupy pro řízení přístupů v rámci sítě 69](#_Toc136334900)

[17.5. Pravidla a postupy pro ochranu vzdáleného přístupu k síti 69](#_Toc136334901)

[17.6. Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů 69](#_Toc136334902)

[18. Politika ochrany před škodlivým kódem 70](#_Toc136334903)

[18.1. Předmět 70](#_Toc136334904)

[18.2. Pravidla a postupy pro ochranu síťové komunikace 70](#_Toc136334905)

[18.3. Pravidla a postupy pro ochranu serverů a sdílených datových úložišť 70](#_Toc136334906)

[18.4. Pravidla a postupy pro ochranu pracovních stanic 70](#_Toc136334907)

[19. Politika bezpečného používání kryptografické ochrany 71](#_Toc136334908)

[19.1. Předmět 71](#_Toc136334909)

[19.2. Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu 71](#_Toc136334910)

[19.3. Pravidla kryptografické ochrany informací 71](#_Toc136334911)

[19.4. Systém správy klíčů 72](#_Toc136334912)

[20. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událost 72](#_Toc136334913)

[20.1. Předmět úpravy 72](#_Toc136334914)

[20.2. Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí 72](#_Toc136334915)

[20.3. Postupy pro vyhodnocování a reakce na detekované kybernetické bezpečnostní události 73](#_Toc136334916)

[20.4. Pravidla pro optimalizaci nastavení nástroje pro detekci kybernetických událostí 73](#_Toc136334917)

[21. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí 74](#_Toc136334918)

[21.1. Předmět 74](#_Toc136334919)

[21.2. Pravidla a postupy pro evidenci a vyhodnocení bezpečnostních událostí 74](#_Toc136334920)

[21.3. Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení bezpečnostních událostí 74](#_Toc136334921)

[21.4. Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení bezpečnostních událostí 75](#_Toc136334922)

## Úvodní ustanovení

Tato směrnice – politika navazuje na směrnici XXXXXX Politika bezpečnosti informací, ve které se Úřad XXXXXX zavázal podporovat ustavení, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování systému řízení bezpečnosti informací.

## Předmět úpravy

1. Účelem této směrnice-politiky je vytvořit rámec pro zavádění organizačních a technických opatření kybernetické bezpečnosti v souladu s požadavky definovanými v:
   * Zákoně 181/2014 Sb. o kybernetické bezpečnosti
   * vyhlášce 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,
   * Vyhlášce č. 360/2020 Sb.Vyhláška, kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb.

## Rozsah platnosti

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

## Pojmy a zkratky

|  |  |  |
| --- | --- | --- |
| **Pojmy** | |  |
| Need to know | | Bezpečnostní zásada, kdy jsou informační aktiva zpřístupněna jen tomu, kdo je potřebuje ke své práci |
| Informace | | Informace snižují míru nejistoty při rozhodování |
| Aktivum primární | | Služba nebo informace, která má pro XXXXXX hodnotu např. tím, že umožňuje plnění zákonných povinností |
| Aktivum podpůrné | | Informační systémy, technologie, budovy, personál atd., na kterých je fungování primárního aktiva závislé |
| SLA | | Service level agreement – smlouva o úrovni služeb – smlouva, která definuje, jakou úroveň mají služby mít. Např. dostupnost informačních systémů, rychlost servisního zásahu apod. |
| RPO | | [Recovery Point Objective](https://www.msp360.com/resources/blog/recovery-point-objective-explained/)  maximální přípustné množství dat, které si instituce může dovolit ztratit během havárie. Pomáhá změřit, jaký čas je únosný mezi poslední zálohou dat a možnou katastrofou |
| RTO | | Recovery Time Objective je metrika, která definuje čas na obnovení IT infrastruktury a služeb po havárii, aby byla zajištěna kontinuita činností instituce |
| BCM | | Business continuity management – sada opatření pro řízení kontinuity činností instituce např. po havárii |
| BCP | | Business continuity plan – sada opatření pro obnovení činnosti např. informačního systému po havárii |
| DRP | | Disaster recovery plan – sada opatření pro obnovení chodu informační infrastruktury |
| CHM | | Change management – postupy pro řízení změn, např. začleňování nových informačních aktiv do informační infrastruktury |
| TLP: WHITE | | TRAFFIC LIGHT PROTOCOL – barevným označením klasifikuje informace a způsoby nakládání s nimi  V souladu se standardními pravidly autorských práv mohou být informace TLP: WHITE šířeny bez omezení. |
| TLP: GREEN | | Příjemci mohou sdílet informace TLP: GREEN s kolegy a partnerskými organizacemi v rámci svého sektoru nebo komunity, ale ne prostřednictvím veřejně přístupných kanálů. |
| TLP: AMBER | | Příjemci mohou sdílet informace TLP: AMBER pouze se členy své vlastní organizace a s klienty nebo zákazníky, kteří tyto informace potřebují znát |
| TLP: RED | | Příjemci nesmí sdílet informace TLP: RED s žádnými stranami mimo konkrétní výměnu, schůzku nebo konverzaci, ve které byly původně zveřejněny |
| Garant aktiva | | Garant aktiva zodpovídá za funkčnost, rozvoj a bezpečnost aktiva. Typicky je to vlastník procesů, jejichž funkčnost aktivum zajišťuje nebo podporuje. |
| Privilegovaný uživatel | | Uživatel s vysokými přístupovými právy k aktivům, typicky administrátor-správce |
| Makro | | Posloupnost kroků, které se mají automaticky vykonat v rámci aplikací MS Office, typicky Word a Excel. Jsou součástí dokumentu a mohou obsahovat škodlivý kód. |
| Akvizice | | Proces získávání či nabytí nějakého aktiva |
| **Zkratky** |  | |
| 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) |
| Sb. | | Sbírka zákonů České republiky |
| ČR | | Česká republika |
| KII | | kritická informační infrastruktura |
| VIS | | významný informační systém |
| PZS | | Poskytovatel základní služby |
| NCKB | | Národní centrum kybernetické bezpečnosti |
| RACI | | Matice odpovědností |
| CERT | | Computer Emergency Response Team |
| IT | | Informační technologie |
| SOC | | dohledové centrum (Security operation Centre) |
| NÚKIB | | Národní úřad pro kybernetickou a informační bezpečnost |
| ISO | | Mezinárodní úřad pro standardizaci |
| IEC | | International Electrotechnical Commission (Mezinárodní elektrotechnická komise) |
| XXXXXX | | XXXXXX |
| SŘBI | | Systém řízení bezpečnosti informací |
| VŘD | | Vnitřní řídící dokumentace |
| BU | | Bezpečnostní událost |
| BI | | Bezpečnostní incident |
| MKB | | Manažer kybernetické bezpečnosti |

## Odpovědnosti a pravomoci

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

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

## Související dokumenty

## Směrnice č. X/XXXX Politika bezpečnosti informací.

## Odpovědnosti a pravomoci

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

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

## Souhrn politik organizačních a technických opatření kybernetické a informační bezpečnosti

Tento dokument je určen k základní orientaci v Politikách organizačních a technických opatření kybernetické a informační bezpečnosti. Stručně popisuje obsah jednotlivých částí – politik. Politiky v plném rozsahu jsou uvedeny v příloze č.1

## Politika systému řízení informační bezpečnosti

definuje:

1. Cíle, principy a potřeby řízení bezpečnosti informací.
2. Rozsah a hranice systému řízení bezpečnosti informací.
3. Pravidla a postupy pro řízení dokumentace.
4. Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací.
5. Pravidla a postupy pro provádění auditů kybernetické bezpečnosti.
6. Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací.
7. Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací.

Primárně je tato politika určena pro vedení XXXXXX, manažera kybernetické bezpečnosti, Odbor informatiky, oddělení personální a mzdové KTA a interní audit.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika systému řízení bezpečnosti informací](#_Politika_systému_řízení)

## Politika organizační bezpečnosti

definuje:

1. Určení bezpečnostních rolí a jejich práv a povinností.
2. Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí.
3. Požadavky na oddělení výkonu bezpečnostních a provozních rolí.

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky a oddělení personální a mzdové KTA.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika organizační bezpečnosti](#_Politika_organizační_bezpečnosti)

## Politika řízení aktiv

definuje :

a) Identifikaci, hodnocení a evidence primárních aktiv

1. určení a evidence jednotlivých primárních aktiv včetně určení jejich garanta, 2. hodnocení důležitosti primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti.

b) Identifikaci, hodnocení a evidence podpůrných aktiv

1. určení a evidence jednotlivých podpůrných aktiv včetně určení jejich garanta, 2. určení vazeb mezi primárními a podpůrnými aktivy.

c) Pravidla ochrany jednotlivých úrovní aktiv

1. způsoby rozlišování jednotlivých úrovní aktiv,

2. pravidla pro manipulaci a evidenci aktiv podle úrovní aktiv,

3. přípustné způsoby používání aktiv.

d) Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií.

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti a Odbor informatiky.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika řízení aktiv](#_Politika_řízení_aktiv)

## Politika řízení dodavatelů

definuje:

a) Pravidla a principy pro výběr dodavatelů.

b) Pravidla pro hodnocení rizik souvisejících s dodavateli.

c) Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.

d) Pravidla pro provádění kontroly zavedení bezpečnostních opatření.

e) Pravidla pro hodnocení dodavatelů.

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky a Odbor KTA (oddělení právní a vymáhání pohledávek a oddělení zadávání veřejných zakázek).

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika řízení dodavatelů](#_Politika_řízení_dodavatelů)

## Politika bezpečnosti lidských zdrojů

definuje:

a) Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení

1. způsoby a formy poučení uživatelů,

2. způsoby a formy poučení garantů aktiv,

3. způsoby a formy poučení administrátorů,

4. způsoby a formy poučení osob zastávajících bezpečnostní role.

b) Bezpečnostní školení nových zaměstnanců.

c) Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací.

d) Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice

1. vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu, 2. změna přístupových oprávnění při změně pracovní pozice.

Primárně je tato politika určena pro XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky a oddělení personální a mzdové KTA.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika bezpečnosti lidských zdrojů](#_Politika_bezpečnosti_lidských)

## Politika řízení provozu a komunikací

definuje:

Jak zajistit spolehlivý, stabilní a bezpečný provoz IS a podpůrných aktiv tak, aby byla zaručena bezpečnost primárních aktiv. Definuje tedy

1. Pravomoci a odpovědnosti spojené s bezpečným provozem
2. Postupy bezpečného provozu
3. Řízení změn
4. Řízení kapacit
5. Oddělení prostředí vývoje, testování a provozu
6. Zaznamenávání událostí
7. Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů

Primárně je tato politika určena pro XXXXXX, pro manažera kybernetické bezpečnosti a Odbor informatiky.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika řízení provozu a komunikací](#_Politika_řízení_provozu)

## Politika řízení změn

definuje:

1. Způsob a principy řízení významných změn v rámci povinné osoby, jejich procesech, informačních a komunikačních systémech.
2. Přezkoumávání dopadů významných změn.
3. Způsob vedení evidence a testování významných změn.

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky a oddělení personální a mzdové KTA.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika řízení změn](#_Politika_řízení_změn)

## Politika řízení přístupu

definuje řízení přístupu k informačním aktivům, zejména:

1. Princip minimálních oprávnění/potřeba znát (need to know).
2. Požadavky na řízení přístupu.
3. Životní cyklus řízení přístupu.
4. Řízení privilegovaných oprávnění.
5. Řízení přístupu pro mimořádné situace.
6. Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky a oddělení personální a mzdové KTA.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika řízení přístupu](#_Politika_řízení_přístupu)

.

## Politika bezpečného chování uživatelů

definuje:

1. Pravidla pro bezpečné nakládání s aktivy.
2. Bezpečné použití přístupového hesla.
3. Bezpečné použití elektronické pošty a přístupu na internet.
4. Bezpečný vzdálený přístup.
5. Bezpečné chování na sociálních sítích.
6. Bezpečnost ve vztahu k mobilním zařízením.

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky i všechny uživatele.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika bezpečného chování uživatelů](#_Politika_bezpečného_chování)

## Politika zálohování a obnovy a dlouhodobého ukládání

definuje:

1. Požadavky na zálohování a obnovu.
2. Pravidla a postupy zálohování.
3. Pravidla a postupy dlouhodobého ukládání.
4. Pravidla bezpečného zálohování a dlouhodobého ukládání informací.
5. Pravidla a postupy obnovy.
6. Pravidla a postupy testování zálohování a obnovy.
7. Politika přístupu k zálohám, ukládaným informacím.

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky i všechny uživatele.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika zálohování a obnovy a dlouhodobého ukládání](#_Politika_zálohování_a)

## Politika bezpečného předávání a výměny informací

definuje:

1. Pravidla a postupy pro ochranu předávaných informací
2. Způsoby ochrany elektronické výměny informací
3. Pravidla pro využívání kryptografické ochrany

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky i všechny uživatele.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika bezpečného předávání a výměny informací](#_Politika_bezpečného_předávání)

## Politika řízení technických zranitelností

definuje:

1. Pravidla pro omezení instalace programového vybavení.
2. Pravidla a postupy vyhledávání opravných programových balíčků.
3. Pravidla a postupy testování oprav programového vybavení.
4. Pravidla a postupy nasazení oprav programového vybavení.

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika řízení technických zranitelností](#_Politika_řízení_technických)

## Politika řízení kontinuity činností

## definuje v případě přerušení činností:

1. Práva a povinnosti zúčastněných osob.
2. Cíle řízení kontinuity činností
   1. minimální úroveň poskytovaných služeb,
   2. doba obnovení chodu,
   3. bod obnovení dat.
3. Politika řízení kontinuity činností pro naplnění cílů kontinuity.
4. Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik.
5. Určení a obsah potřebných plánů kontinuity a havarijních plánů.
6. Postupy pro realizaci opatření vydaných Úřadem.

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky, Oddělení právní a vymáhání pohledávek, Odbor vnějších vztahů a kultury.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika řízení kontinuity činností](#_Politika_řízení_kontinuity)

## Politika zvládání kybernetických bezpečnostních incidentů

definuje:

a) kategorie kybernetického bezpečnostního incidentu.

b) Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů.

c) Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů.

d) Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti.

e) Pravidla evidence incidentů.

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky, Oddělení právní a vymáhání pohledávek, Odbor vnějších vztahů a kultury.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika zvládání kybernetických bezpečnostních incidentů](#_Politika_zvládání_kybernetických)

## Politika akvizice, vývoje a údržby

definuje:

1. Bezpečnostní požadavky pro akvizici, vývoj a údržbu
2. Řízení zranitelností
3. Poskytování a nabývání licencí programového vybavení a informací

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky, Oddělení právní a vymáhání pohledávek.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika akvizice, vývoje a údržby](#_Politika_akvizice,_vývoje)

## Politika fyzické bezpečnosti

definuje:

1. Pravidla pro ochranu objektů
2. Pravidla pro kontrolu vstupu osob
3. Pravidla pro ochranu zařízení
4. Detekce narušení fyzické bezpečnosti

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky, Odbor XXX, Odbor správy majetku.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika fyzické bezpečnosti](#_Politika_fyzické_bezpečnosti)

## Politika bezpečnosti komunikační sítě

definuje:

1. Pravidla a postupy pro zajištění bezpečnosti sítě
2. Určení práv a povinností za bezpečný provoz sítě
3. Pravidla a postupy pro řízení přístupů v rámci sítě
4. Pravidla a postupy pro ochranu vzdáleného přístupu k síti
5. Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika bezpečnosti komunikační sítě](#_Politika_bezpečnosti_komunikační)

## Politika ochrany před škodlivým kódem

definuje:

1. Pravidla a postupy pro ochranu síťové komunikace
2. Pravidla a postupy pro ochranu serverů a sdílených datových úložišť
3. Pravidla a postupy pro ochranu pracovních stanic

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky,

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika ochrany před škodlivým kódem](#_Politika_ochrany_před)

## Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

definuje:

1. Pravidla a postupy nasazení nástroje pro detekci   
   kybernetických bezpečnostních událostí
2. Provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události
3. Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událost](#_Politika_nasazení_a)

## Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

definuje:

1. Pravidla a postupy pro evidenci a vyhodnocení   
   bezpečnostních událostí
2. Pravidla a postupy pravidelné aktualizace pravidel   
   pro vyhodnocení bezpečnostních událostí
3. Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení bezpečnostních událostí

Primárně je tato politika určena pro vedení XXXXXX, pro manažera kybernetické bezpečnosti, Odbor informatiky.

Plné znění této politiky je uvedeno v Příloze č.1 zde: [Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí](#_Politika_využití_a)

## Příloha č.1

## Politika systému řízení bezpečnosti informací

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je:

* 1. definovat cíl, principy a potřeby řízení bezpečnosti informací,
  2. stanovit rozsah a hranice systému řízení,
  3. definovat pravidla a postupy nutné pro naplnění těchto cílů a principů.

### Cíle, principy a potřeby řízení bezpečnosti informací

1. Cílem řízení bezpečnosti informací je zajištění důvěrnosti informací ve všech formách jejich výskytu (informace je přístupná jen těm, kteří jsou oprávněni mít k ní přístup), zajištění dostupnosti (informace a s nimi spojená aktiva jsou uživatelům přístupná v době, kdy je potřebují) a zabezpečení integrity (přesnost a kompletnost informací a metod jejich zpracování).
2. SŘBI si klade za cíl zabezpečit ochranu informací v celé jejich šíři a ve všech formách pomocí přiměřených a odpovídajících opatření, která budou chránit aktiva tak, aby poskytla odpovídající míru jistoty všech zainteresovaných subjektů. Tento cíl je naplňován vybudováním, zavedením, provozováním, kontrolováním, údržbou a neustálým zlepšováním dokumentovaného SŘBI založeném na přístupu k řízení rizik v kontextu XXXXXX.
3. Revize cíle SŘBI je prováděna v závislosti na platných právních předpisech, na výsledcích Auditů a změnách cílů činnosti XXXXXX.
4. Principy řízení bezpečnosti informací vycházejí z obecně platného pravidla, že jedině u řízené a koordinované činnosti lze očekávat synergický efekt bezpečnostních opatření, a jsou následující:
   1. **Princip need-to-know** znamená, že přístup a rozsah oprávnění zaměstnance nebo dotčené třetí strany má být odvozen od toho, co potřebuje znát pro výkon práce.
   2. **Princip kompaktnosti a úplného pokrytí** znamená, že bezpečnost informací je tak odolná, jak odolný je její nejslabší článek. Bezpečnost informací musí být navrhována tak, aby působila vyváženě a chránila všechna aktiva. Zásady bezpečnosti informací musí být jednotně prosazovány do všech činností a procesů.
   3. **Princip přiměřenosti** znamená, že bezpečnostní opatření musí být navržena tak, aby odpovídala velikosti rizika a hodnotě aktiv, která chrání.
   4. **Princip koordinace bezpečnosti** znamená, že bezpečnostní působení v rámci ochrany informací musí být koordinované, aby se zabezpečil soulad a návaznost jednotlivých bezpečnostních opatření.
   5. **Princip řízení bezpečnostní dokumentace** znamená, že postupy a procesy musí být dokumentovány, aby byla zachována jejich přesná opakovatelnost a dohledatelnost. Tato dokumentace je průběžně aktualizována. O bezpečnostních událostech se vedou záznamy.
   6. **Princip soustavného rozvoje** je založen na sledování, měření a vyhodnocování efektivnosti systému bezpečnosti, jeho přezkoumávání a soustavném zlepšování. Cílem je trvalý rozvoj kybernetické bezpečnosti, zkvalitňování poskytovaných služeb a zvyšování úrovně zajištění IS.
   7. **Princip odpovědnosti** znamená, že prosazení stanovených zásad, pravidel a postupů SŘBI je vždy na všech úrovních řízení v souladu s deklarovanými cíli a spojeno s individuální odpovědností jednotlivých osob.
   8. **Princip integrace** znamená, že prosazování bezpečnosti informací je řízeno komplexním SŘBI, který integruje a koordinuje činnosti všech dotčených útvarů i zúčastněných třetích stran.
   9. **Princip souladu s právními předpisy** znamená, že všechny zásady, pravidla a postupy jsou v souladu s právními předpisy závaznými pro XXXXXX a relevantními technickými normami a jsou v souladu s uzavřenými smluvními závazky.
   10. **Princip bezpečnostního povědomí** znamená poučení o bezpečném nakládání s informacemi, jejich vytváření a zpracování.
   11. **Princip formalizace** znamená, že prosazování a řízení bezpečnosti informací je spojeno s formalizovanými, jednoznačně definovanými a náležitě popsanými postupy, jejichž uplatňování je řádně dokumentováno. Nedílnou součástí řízení jsou nástroje kontroly a nezávislého auditu, které důsledně ověřují míru a kvalitu skutečné realizace všech přijatých opatření.
   12. **Princip nepřetržitosti** znamená průběžnou identifikaci bezpečnostních událostí a incidentů a přijímání přiměřeně účinných bezpečnostních opatření pro zajištění bezpečnosti informací. Tento princip je uplatňován nepřetržitě na všech aktivech.
   13. **Princip řízení rizik** znamená, že rizika jsou průběžně vyhodnocována, je stanovována jejich akceptovatelná úroveň. Rizika jsou zvládána zaváděním vhodných opatření tak, aby byla dosažena požadovaná úroveň bezpečnosti informací a zajištěna kontinuita činností.
   14. **Princip důvěrnosti, integrity a dostupnosti** znamená, že informace jsou přístupné jen autorizovaným jednotlivcům, entitám nebo procesům, jsou platné, konzistentní a přesné v průběhu celého životního cyklu, přístupné v čase a místě dle potřeb XXXXXX.
5. Potřeby řízení bezpečnosti informací vyplývají z hodnocení aktiv a rizik. V rámci tohoto procesu jsou zhodnoceny hrozby, zranitelnosti a úrovně jednotlivých rizik. Následně jsou definována patřičná nápravná opatření.

### Rozsah a hranice systému řízení bezpečnosti informací

1. Rozsah SŘBI je stanoven bezpečnostními politikami, pravidly a další bezpečnostní dokumentací.
2. Celková hranice SŘBI je definována jako množina všech hranic aktiv XXXXXX, vzhledem k:
   1. klíčovým informačním aktivům XXXXXX jako poskytovatele základní služby ve smyslu zákona 181/2014 Sb. o kybernetické bezpečnosti a návazných předpisů.
   2. provázanostem a návaznostem ostatních aktiv
   3. zajištění jednotných bezpečnostních pravidel a opatření,
   4. hospodárnosti, účelnost a efektivitě při řízení bezpečnosti informací.
3. S ohledem na výše stanovenou hranici SŘBI a na princip přiměřenosti mohou být jednotlivá aktiva chráněna rozdílným stupněm zabezpečení.

### Pravidla a postupy pro řízení dokumentace

1. Výchozím dokumentem SŘBI je interní akt řízení, kterým se zřizuje Výbor pro řízení kybernetické bezpečnosti (dále jen „Výbor“), stanoví základní bezpečnostní role a ukládá Výboru základní práva a povinnosti.

1. Základním řídícím dokumentem SŘBI je tato směrnice (včetně bezpečnostních politik), která stanovuje hlavní zásady SŘBI. Gestorem směrnice je Manažer KB, který věcnou stránku zajišťuje ve spolupráci s osobami zastávajícími bezpečnostní role a s příslušnými útvary.
2. Dokumentace SŘBI je rozdělena na dílčí části, které odpovídají oblastem řízení bezpečnosti. Dokumentace SŘBI je dále členěna na:
3. **Politiky** – vrcholové dokumenty schválené vedením XXXXXX specifikující pokyny pro řízení SŘBI na strategické úrovni. Jsou v gesci tajemníka úřadu a vedeny v systému vnitřních organizačních předpisů úřadu, ve Znalostní bázi XXXXXX na Intranetu.
4. **Standardy** – konkrétní a povinná pravidla, která podporují politiky. Jsou v gesci MKB a garanta příslušného aktiva
5. **Metodické postupy** – detailní postupy a metodiky pro dané činnosti na taktické úrovni. Jsou v gesci MKB a administrátora příslušného aktiva nebo skupiny aktiv, pokud je lze seskupit.
6. **Provozní záznamy** – záznamy o provozu a řízení SŘBI. Jsou v gesci MKB a administrátora
7. Dostupnost dokumentace:
8. bezpečnostní politiky jsou dostupné všem zaměstnancům XXXXXX
9. bezpečnostní politiky jsou uloženy v elektronické i listinné podobě. V elektronické podobě jsou dostupné na Intranetu XXXXXX
10. další bezpečnostní dokumentace je dostupná pouze určeným osobám, zejména osobám zastávajícím bezpečnostní role, a to v rozsahu, který přísluší dané roli,
11. veškerá bezpečnostní dokumentace bude v budoucnu vedena na nově zřízeném Portálu informační bezpečnosti.
12. Označování dokumentace:
13. dokument je označován a evidován v souladu s vnitřním organizačním předpisem XXXXXX Spisovým řád.
14. pravidla pro označování a evidenci dokumentů konkrétního prvku ICT jsou součástí dokumentace daného prvku. Každý prvek nebo skupina prvků se stejnými vlastnostmi má svoji provozní, uživatelskou a bezpečnostní dokumentaci.
15. Tvorba a změny bezpečnostní dokumentace na Intranetu resp. v budoucnu na Portálu informační bezpečnosti:
16. tvorbu a revizi dokumentu zabezpečuje Garant aktiva, který současně odpovídá za jeho platnost,
17. revize dokumentu se provádí minimálně jednou ročně a při každé změně bezpečnostních parametrů aktiva
18. publikování dokumentů zajišťuje Manažer KB (publikování dokumentů je až na výjimky ve formátu PDF/A)
19. informování o změně dokumentu nebo o vydání nového dokumentu zajišťuje Garant aktiva.
20. Za uložení, umožnění nebo omezení přístupu a ochranu platné bezpečnostní dokumentace je odpovědný příslušný Garant aktiva, ke kterému se bezpečnostní dokumentace vztahuje.

### Pravidla a postupy řízení provozu a zdrojů systému řízení bezpečnosti informací

1. SŘBI je rozdělen do čtyř fází (cyklus PDCA), které běží kontinuálně s cílem neustálého zlepšování vhodnosti, přiměřenosti a účinnosti SŘBI:
2. Plánování (Plan),
3. Provedení (Do),
4. Kontrola (Check),
5. Akce (Act).
6. Ve fázi „Plánování“ je řešeno:
7. nastavení procesu, jehož vstupem je rozhodnutí o vybudování nebo modifikaci SŘBI,
8. zpracování bezpečnostní dokumentace vztahující se k SŘBI, zejména bezpečnostních politik ve smyslu zvláštního právního předpisu[[1]](#footnote-1)) a jejich aktualizace v následujících cyklech,
9. zpracování výstupů z fáze „Akce“ z předcházejícího cyklu,
10. plánování zdrojů,
11. zpracování požadavků na změny a opatření související se zlepšováním účinnosti SŘBI nebo vynucené zaváděním nových opatření spadajících do této oblasti,
12. zpracování požadavků provedených kontrol a auditů kybernetické bezpečnosti.
13. Ve fázi „Provedení“ je řešeno:
14. zavedení nebo modifikace řízení SŘBI,
15. monitorování bezpečnostních událostí a incidentů,
16. aplikace bezpečnostních politik a bezpečnostních opatření z předcházející fáze „Plánování“.
17. Ve fázi „Kontrola“ je řešeno:
18. vyhodnocení fáze „Provedení“,
19. identifikování zranitelností v procesu řízení kybernetické bezpečnosti,
20. řízení kontrolní činnosti,
21. provádění auditu kybernetické bezpečnosti,
22. vyhodnocení rizik a identifikace nových rizik.
23. Ve fázi „Akce“ je řešeno:
24. vyhodnocení fáze „Kontrola“ a „Provedení“,
25. přezkoumání a vyhodnocení účinnosti SŘBI,
26. navržení bezpečnostních opatření a definování požadavků na zlepšování SŘBI.

### Pravidla a postupy pro provádění auditů kybernetické bezpečnosti

Audit kybernetické bezpečnosti posuzuje soulad bezpečnostních opatření s právními předpisy, interními akty řízení a smluvními závazky vztahujícími se zejména VIS.

### Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací

1. Přezkoumání SŘBI hodnotí možnosti zlepšení a potřebu změn, včetně potřeby aktualizovat bezpečnostní dokumentaci, cíle bezpečnosti a hodnocení aktiv a rizik.
2. Přezkoumání SŘBI vytyčuje nové cíle pro další cykly a zachovává stálou či stoupající úroveň efektivnosti SŘBI. Výsledky přezkoumání jsou dokumentovány a jsou uchovávány.
3. Manažer KB z podkladů a doporučení získaných z fází cyklu PDCA zpracovává a předkládá „Zprávu o přezkoumání SŘBI“ Výboru minimálně jednou ročně. „Zpráva o přezkoumání SŘBI“ zahrnuje např. výsledky auditů a kontrol, výsledky předchozího přezkoumání, výsledky přezkoumání, stav bezpečnostních opatření, zranitelnosti a hrozby, důležité změny, doporučení pro zlepšení, návrh rozhodnutí k zvyšování účinnosti SŘBI, návrh rozhodnutí k aktualizaci „Plánu zvládání rizik“, návrh rozhodnutí ke změně bezpečnostní dokumentace a postupů v reakci na změny vnitřních i vnějších podmínek a návrh rozhodnutí k potřebě finančních i jiných zdrojů.
4. Zaměstnanci, podílející se na řízení SŘBI, se podílí na průběžném přezkoumávání celého SŘBI.
5. Vedoucí zaměstnanci v rámci své řídící a kontrolní činnosti dohlíží na to, aby zaměstnanci v jejich řízeném útvaru vykonávali činnosti v souladu s principy a zásadami SŘBI a o zjištěných závažných porušeních principů a zásad SŘBI jsou povinni informovat MKB.

### Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací

1. Po schválení nápravných opatření a návrhů na zlepšení Manažer KB zahájí jejich realizaci zadáním požadavků do nástroje podporujícího řízení SŘBI.
2. Řešitel požadavku průběžně informuje o postupu činností v realizaci nápravných opatření prostřednictvím nástroje podporujícího řízení SŘBI.

## Politika organizační bezpečnosti

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti, která vychází z požadavků zvláštního právního předpisu[[2]](#footnote-2)), je:

1. stanovit a popsat bezpečnostní role, které jsou součástí organizační struktury systému řízení bezpečnosti informací, a určit jejich povinnosti a odpovědnosti,
2. definovat způsoby určení bezpečnostních rolí,
3. popsat vzájemné vztahy jednotlivých bezpečnostních rolí.

### Rozsah působnosti

1. Politika organizační bezpečnosti se vztahuje zejména na:
   1. Výbor pro řízení kybernetické bezpečnosti,
   2. bezpečnostní role:
      1. Manažer KB,
      2. Architekt KB,
      3. Auditor KB,
      4. Garant primárních aktiv,
      5. Garant podpůrných aktiv,
      6. Bezpečnostní správce,
      7. Administrátor,
   3. vedoucí zaměstnance,
   4. uživatele,
   5. ostatní role v oblasti bezpečnosti, tedy na pracovníky (tj. interní zaměstnanci MČP5 nebo pracovníky smluvních stran) zastávající role definované v bezpečnostní dokumentaci všech úrovní,
   6. dodavatele nebo partnery dodávající zboží a nebo zajišťující služby, které mají vliv na prvky kybernetické a informační bezpečnosti MČP5.
2. Zaměstnanci, kteří zastávají bezpečnostní role, mohou svými právy a povinnostmi prokazatelně pověřit jiného zaměstnance.
3. Role SŘBI zastávají zaměstnanci nebo smluvní strany, kterým jsou přiřazena konkrétní práva a povinnosti v rámci SŘBI.

### Určení bezpečnostních rolí

1. Povinnost zřízení Výboru pro řízení kybernetické bezpečnosti a ustanovení MKB, Architekta KB, Garantů aktiv a Auditora KB se řídí zvláštním právním předpisem**[[3]](#footnote-3)**). Určení členů Výboru pro řízení kybernetické bezpečnosti, MKB, Architekta KB a Auditora KB provádí starosta interním aktem řízení upravujícím zřízení Výboru a stanovení bezpečnostních rolí.
2. Jmenování zaměstnance k zastávání bezpečnostní role a jeho odvolání musí být vždy prokazatelné. Jmenovací listiny jsou ukládány v personální složce příslušného zaměstnance.
3. Manažer KB, Architekt KB a Auditor KB jsou prokazatelně jmenováni a odvoláváni starostou.
4. Zaměstnanci zastávající bezpečnostní role Manažer KB a Architekt KB musí mít prokazatelně jmenovaného zástupce.
5. Garanti primárních aktiv jsou na návrh předsedy Výboru pro řízení kybernetické bezpečnosti prokazatelně jmenováni a odvoláváni starostou. Obecně platí, že Garantem primárního aktiva je vedoucí útvaru, který primární aktivum (tj. službu nebo informaci) využívá pro svou činnost.
6. Garanty podpůrných aktiv navrhuje Manažer KB ve spolupráci s Garanty primárních aktiv prokazatelně je jmenuje a odvolává předseda Výboru pro řízení kybernetické bezpečnosti. Obecně platí, že Garantem podpůrných aktiv je vedoucí oddělení mající daná podpůrná aktiva ve správě. Pro potřeby snazší správy je možné podpůrná aktiva sdružovat a určit jim pouze jednoho garanta aktiva, respektive skupiny aktiv.
7. Zaměstnanci, kteří zastávají bezpečnostní role, mohou svými právy a povinnostmi prokazatelně pověřit jiného zaměstnance. Vlastní bezpečnostní role a konečná odpovědnost však zůstává na zaměstnanci, který byl do bezpečnostní role jmenován.

### Výbor pro řízení kybernetické bezpečnosti, jeho práva a povinnosti

1. Pravomoci a odpovědnosti členů Výboru pro řízení kybernetické bezpečnosti jsou stanoveny Jednacím řádem Výboru pro řízení kybernetické bezpečnosti.
2. Výbor pro řízení kybernetické bezpečnosti koordinuje plánování opatření k zajišťování bezpečnosti informací.
3. Výbor pro řízení kybernetické bezpečnosti v rámci své působnosti zejména:
   1. odpovídá za celkové řízení a rozvoj SŘBI XXXXXX,
   2. definuje strategické cíle a směřování rozvoje bezpečnosti informací a koordinuje přípravu a implementaci SŘBI v XXXXXX,
   3. posuzuje a projednává bezpečnostní dokumentaci,
   4. definuje role a odpovědnosti v rámci SŘBI, včetně ustanovení pracovních skupin v rámci SŘBI,
   5. schvaluje významné výstupy SŘBI (např. katalog rizik) a průběžně kontroluje a dohlíží na provozní aspekty SŘBI (např. správu bezpečnostních incidentů, správu významných změn a dodavatelů a podobně),
   6. schvaluje návrhy a implementace významných bezpečnostních opatření v XXXXXX vyžadujících rozsáhlé změny, včetně stanovení útvarů spoluodpovědných za implementaci opatření a předběžné termíny a odhad nákladů na implementaci vybraných opatření,
   7. vyhodnocuje stav a účinnost SŘBI v organizaci na základě provedených kontrol a auditů kybernetické bezpečnosti,
   8. definuje požadavky na podávání zpráv a měřitelné požadavky na kontrolu SŘBI,
   9. pomáhá zajistit součinnost jednotlivých útvarů při prosazování SŘBI ve MČP5,
   10. podporuje vzdělávání v oblasti SŘBI ve MČP5,
   11. zabezpečuje koordinaci plánovacích a přípravných aktivit v oblasti zajišťování bezpečnosti informací důležitých pro stabilitu a bezpečnost s důrazem na ochranu KII a VIS,
   12. posuzuje a projednává požadavky na zdroje uplatňované v rámci zajišťování bezpečnosti informací a plnění plánovaných cílů,
   13. projednává seznamy primárních aktiv, KII a VIS,
   14. projednává návrh na jmenování nebo odvolání Garantů primárních aktiv,
   15. projednává zprávy z auditu kybernetické bezpečnosti a na základě rozhodnutí předsedy Výboru pro řízení kybernetické bezpečnosti ukládá přijmout opatření ke zjištěným nedostatkům členům Výboru pro řízení kybernetické bezpečnosti v rozsahu jejich působnosti.

### Manažer kybernetické bezpečnosti, jeho práva a povinnosti

1. Manažer KB je zaměstnanec odpovědný za řízení SŘBI.
2. Manažer KB je oprávněn navrhovat organizační opatření upravující činnosti obecně organizačního, administrativního nebo technického charakteru, včetně bezpečnostních aspektů.
3. Klíčové činnosti MKB jsou:
   1. odpovědnost za řízení SŘBI,
   2. předkládání Výboru pro řízení kybernetické bezpečnosti k projednání Zprávy z přezkoumání SŘBI, Zprávy o hodnocení aktiv a rizik, Plánu zvládání rizik, Prohlášení o aplikovatelnosti a Plán rozvoje bezpečnostního povědomí,
   3. poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti ICT (zejména definuje bezpečnostní požadavky na dodavatele),
   4. komunikace s Úřadem[[4]](#footnote-4)),
   5. podílení se na procesu řízení rizik,
   6. koordinace řízení bezpečnostních incidentů,
   7. vyhodnocování vhodnosti a účinnosti bezpečnostních opatření,
   8. definování taktických a operativních cílů SŘBI,
   9. definování vhodných bezpečnostních požadavků a opatření pro jednotlivá IT prostředí a typy aktiv ve spolupráci s Architektem KB a dohled nad realizací bezpečnostních opatření,
   10. stanovení postupů hodnocení a řešení bezpečnostních událostí (BU) a bezpečnostních incidentů (BI),
   11. provádění přezkoumání a kontroly bezpečnostní dokumentace,
   12. řízení přidělených bezpečnostních projektů po technické a organizační stránce,
   13. zpracování metodických materiálů v rámci své působnosti (zejména metodiky pro identifikaci a hodnocení aktiv a rizik a vybraných bezpečnostních politik, resp. metodických postupů k této směrnici),
   14. návrh nápravných opatření zjištěných nedostatků při řízení SŘBI a zjištěných BU a BI,
   15. projednávání, nahlašování a aktualizace systémů, spadajících pod působnost Úřadu
   16. komunikace s Úřadem při řešení možných zranitelností a hrozeb, včetně kontroly realizace nápravných opatření,
   17. zajištění bezodkladného hlášení BI Úřadu5).
   18. odpovědnost za vytvoření a vedení aktuální a úplné evidence primárních aktiv.

### Architekt kybernetické bezpečnosti, jeho práva a povinnosti

1. Architekt KB je odpovědný za návrh implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura XXXXXX.
2. Architekt KB zajišťuje bezpečnou architekturu:
   1. prováděním kontrol, hodnocení a testování funkčnosti zavedených bezpečnostních opatření,
   2. vytvářením testovacích postupů a odpovídající kritéria akceptace,
   3. definováním bezpečnostních požadavků na architektonické úrovni při návrhu, vývoji, testování a implementaci nových informačních a komunikačních systémů a změnu stávajících,
   4. navrhováním a optimalizováním opatření a procesů řešení BU a BI.
3. Architekt KB analyzuje architekturu SŘBI, jeho jednotlivých komponent, včetně vzájemných vazeb a zodpovídá za tvorbu a údržbu procesně-organizačního a aplikačního modelu architektury bezpečnosti informací.

### Auditor kybernetické bezpečnosti, jeho práva a povinnosti

1. Auditor KB je odpovědný za provádění auditu kybernetické bezpečnosti.
2. Práva a povinnosti Auditora KB jsou definovány ve Statutu interního auditu.
3. Auditor KB nesmí být stálým členem Výboru pro řízení kybernetické bezpečnosti, avšak je oprávněn se účastnit zasedání Výboru pro řízení kybernetické bezpečnosti a vyžadovat zápisy ze zasedání.
4. Role Auditora KB je oddělena od výkonu dalších bezpečnostních rolí a není slučitelná s rolemi odpovědnými za provoz IS.
5. Auditor KB posuzuje soulad implementovaných bezpečnostních opatření v MČP5 s nejlepší praxí, právními předpisy, interními akty řízení, jinými předpisy a smluvními závazky vztahujícími se k prvku KII či VIS, včetně přezkoumání technické shody a dává doporučení pro zajištění souladu s legislativními požadavky.

### Garant primárního aktiva, jeho práva a povinnosti

1. Garant primárního aktiva je odpovědný za zajištění rozvoje, použití a bezpečnosti primárního aktiva.
2. Každé primární aktivum musí mít přiděleno svého Garanta.
3. Garant primárního aktiva ve spolupráci s garantem podpůrného a MKB:
   1. Poskytuje podklady MKB analýzu rizik pro dané primární aktivum za podpory MKB,
   2. Ve spolupráci s MKB stanoví hodnotu aktiva z pohledu důvěrnosti, integrity a dostupnosti primárního aktiva,
   3. stanovuje obecné bezpečnostní požadavky a koncepty (např. požadované doby obnovy, matici přístupu k primárnímu aktivu či další požadavky na bezpečné užívání, provoz a rozvoj) pro dané primární aktivum na základě klasifikace,
   4. na základě návrhů MKB, Garanta podpůrného aktiva či bezpečnostního správce schvaluje navržená bezpečnostní pravidla a opatření řešící bezpečnostní požadavky pro dané primární aktivum, respektive související podpůrné aktivum typu aplikační služba,
   5. Zodpovídá za použití, rozvoj a bezpečnost aktiva informuje MKB o všech změnách aktiva, které mohou nebo mají vliv na hodnotu aktiva

### Garant podpůrného aktiva, jeho práva a povinnosti

1. Garant podpůrného aktiva je odpovědný za zajištění rozvoje, použití a bezpečnosti podpůrného aktiva.
2. Každé podpůrné aktivum musí mít přiděleno svého Garanta.
3. Garant podpůrného aktiva:
   1. provádí hodnocení důvěrnosti, integrity a dostupnosti podpůrného aktiva, a to na základě primárního aktiva či nadřazených technologických vrstev podpůrných aktiv, které dané aktivum podporuje,
   2. v souladu s bezpečnostními požadavky a bezpečnostní dokumentací zajistí realizaci bezpečnostních opatření,
   3. zajištuje správu podpůrného aktiva a je odpovědný za jeho užívání v souladu s bezpečnostními požadavky a dokumentací a v souladu s přidělenou rolí,
   4. informuje MKB o všech změnách aktiva, které mohou nebo mají vliv na hodnotu aktiva podpůrného aktiva,
   5. informuje Garanty příslušných podpůrných aktiv nadřazených technologických vrstev.

### Bezpečnostní správce, jeho práva a povinnosti

1. Bezpečnostní správce zodpovídá za řízení, prosazování a kontrolu bezpečnosti informací v rámci svěřeného aktiva.
2. Bezpečnostní správce udržuje aktuální seznam oprávněných uživatelů s jejich přidělenými přístupovými oprávněními.
3. Bezpečnostní správce stanoví pravidla pro mazání dat a likvidaci technických nosičů dat v souladu se zvláštním právním předpisem[[5]](#footnote-5)).
4. Zajišťuje kontrolu dodržování zákonných a licenčních podmínek z hlediska využívání programového vybavení.
5. Bezpečnostní správce provádí:
   1. správu a evidenci konfigurace HW i SW, vede přehled umístění všech zařízení,
   2. zálohování systémového programového vybavení a konfigurací a zajišťuje ochranu záložních médií,
   3. správu a evidenci jím zpracované nebo mu svěřené bezpečnostní dokumentace,
   4. kontrolu auditních záznamů ve shodě s bezpečnostní dokumentací,
   5. archivní kopie auditních záznamů (logů).

### Administrátor informačních systémů a technologií, jeho práva a povinnosti

1. Administrátor zajišťuje správu, provoz, použití a bezpečnost technického aktiva.
2. Administrátor je odpovědný za realizaci bezpečnostních opatření v provozu ICT.
3. Administrátor vykonává pokyny Garanta příslušného aktiva, poskytuje součinnost Garantovi podpůrného aktiva a Bezpečnostnímu správci.

### Bezpečnostní procesy pro bezpečnostní role kybernetické bezpečnosti

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

1. R (Responsible) - má odpovědnost za přímé provádění daného úkolu,
2. A (Accountable) - má odpovědnost za to, že daný proces je vykonáván v souladu se schválenou podobou procesu,
3. C (Consulted ) - spolupracuje na procesu,
4. I (Informed) - je informován o výsledku jednotlivých fází procesu.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Oblast** | **ROLE** | | | | | | | |
| **Výbor pro řízení kybernetické bezpečnosti** | **Manažer KB** | **Architekt KB** | **Auditor KB** | **Garant primárního aktiva** | **Garant podpůrného aktiva** | **Bezpečnostní správce** | **Administrátor** |
| **Řízení kybernetické bezpečnosti** | **A** | **R** | **R/C** | **I** | **R** | **R** | **R** | **R** |
| **Audit kybernetické bezpečnosti** | **I** | **C/ I** | **C/I** | **A/ R** | **C / I** | **C / I** | **C/ I** | **C / I** |
| **Návrh bezpečnostních opatření** | **A** | **R** | **R** | **I** | **C** | **C** | **C** | **C** |
| **Realizace bezpečnostních opatření** | **I** | **A** | **C** | **I** | **R** | **R** | **A** | **R** |
| **Zajištění rozvoje, použití a bezpečnosti primárního aktiva** | **I** | **C** | **C** | **-** | **A** | **R** | **C** | **R** |
| **Zajištění rozvoje, použití a bezpečnosti podpůrného aktiva** | **I** | **C** | **C** | **-** | **C** | **A** | **C** | **R** |

### Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí

1. Povinnosti a vymezení působnosti jednotlivých rolí SŘBI musí být z důvodu střetu zájmů odděleny, aby se omezily příležitosti pro neoprávněné nebo neúmyslné změny nebo zneužití aktiv.
2. Zaměstnanec nemůže být současně jmenován do bezpečnostní role MKB a Garanta aktiva.
3. Role MKB a Architekta KB nejsou slučitelné s rolemi odpovědnými za provoz ICT.
4. Zaměstnanec zastávající bezpečnostní roli Auditora KB nesmí být současně jmenován do žádné jiné bezpečnostní role. Jeho role není slučitelná s rolemi odpovědnými za provoz ICT.
5. Bezpečnostní správce nesmí být Administrátor nebo Garant stejného aktiva, Architekt KB, Manažer KB.

## Politika řízení aktiv

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je:

* 1. definovat systém klasifikace primárních aktiv,
  2. definovat způsob určení a jmenování Garantů aktiv,
  3. provést identifikaci, hodnocení a evidenci primárních a podpůrných aktiv,
  4. určit vazby mezi primárními a podpůrnými aktivy,
  5. definovat pravidla ochrany aktiv,
  6. definovat způsoby likvidace technických i jiných nosičů dat,
  7. definovat způsoby a standardy pro kompletní smazání dat v případě předání zařízení jinému uživateli, jejich prodeji, darování nebo likvidaci.

K hodnocení aktiv je vydávána metodika, která je zveřejněna na Intranetu a v budoucnu na Portále informační bezpečnosti.

### Rozdělení aktiv

1. Identifikace aktiv a jejich následná analýza je základním předpokladem pro efektivní řízení jejich bezpečnosti v rámci SŘBI.
2. Primárním aktivem se pro účely SŘBI rozumí informace nebo služby.
3. Mezi podpůrná aktiva se řadí:
   1. technická aktiva (technické vybavení, komunikační prostředky a programové vybavení apod.),
   2. objekty,
   3. zaměstnanci,
   4. dodavatel podílející se na provozu, rozvoji, správě nebo bezpečnosti IS.
4. Každé aktivum má určeno svého Garanta.

### Garant aktiva

1. Garant aktiva je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnosti aktiva[[6]](#footnote-6)).
2. Garanti primárních aktiv jsou na návrh předsedy Výboru jmenováni a odvoláváni tajemníkem XXXXXX.
3. Garanty podpůrných aktiv navrhuje Manažer KB ve spolupráci s Garantem primárního aktiva a jmenuje a odvolává předseda Výboru.
4. Garant primárního aktiva ve spolupráci s garantem podpůrného aktiva a Manažerem KB odpovídá za:
   1. zajištění klasifikace a hodnocení aktiva,
   2. definici požadavků na bezpečnost aktiva (v souladu s hodnotou aktiva a úrovní poskytované služby),
   3. definici omezení přístupu k aktivu,
   4. definici požadavků na správu aktiva a jeho užívání,
   5. pravidelný přezkum omezení přístupu k aktivu a přezkum klasifikace aktiva
   6. identifikaci podpůrných aktiv ve spolupráci s Manažerem KB,
   7. analýzu rizik ve spolupráci s Manažerem KB.
5. Garant podpůrného aktiva odpovídá za:
   1. zajištění klasifikace a hodnocení aktiva,
   2. definici požadavků na bezpečnost aktiva,
   3. definici omezení přístupu k aktivu,
   4. zajištění správy aktiva a jeho užívání v souladu s bezpečnostními požadavky a dokumentací,
   5. pravidelný přezkum omezení přístupu k aktivu a přezkum klasifikace aktiva
   6. analýzu rizik ve spolupráci s Manažerem KB.
6. Veškerá primární a podpůrná aktiva XXXXXX musí mít přiřazeného svého Garanta.
7. Zaměstnanci, kteří zastávají bezpečnostní role, mohou svými právy a povinnostmi prokazatelně pověřit jiného zaměstnance. Vlastní bezpečnostní role a odpovědnost zůstává na zaměstnanci, který byl do této role jmenován.

### Identifikace primárních aktiv

1. Manažer KB ve spolupráci s ostatními zaměstnanci identifikuje primární aktiva.
2. Manažer KB předloží Výboru k projednání návrh na určení Garantů primárních aktiv.
3. Primární aktiva jsou identifikována zejména dle těchto principů:
   1. tvoří logický koncept, který je možné popsat,
   2. jsou rozpoznána/pojmenována nezávisle na konkrétním IS,
   3. jsou využívána v rámci hlavních nebo rozhodovacích procesů,
   4. podléhají životnímu cyklu,
   5. jsou definována na takové úrovni detailu, že je možné jejich součásti spravovat jako ucelené jednotky,
   6. informace obsažené ve dvou různých druzích datových sad představují dvě samostatná primární aktiva.

### Hodnocení primárních aktiv

1. Hodnocení identifikovaných primárních aktiv je řízeno a dokumentováno.
2. Hodnocení provede Garant primárního aktiva ve spolupráci s Manažerem KB.
3. Hodnocení primárních aktiv probíhá minimálně na úrovni zajištění:
   1. důvěrnosti,
   2. integrity,
   3. dostupnosti.
4. Hodnocení důvěrnosti je provedeno na stupnici dle Tabulky č. 1:

| **Úroveň** | | **Popis** |
| --- | --- | --- |
| 1 | Nízká | Aktivum je veřejně přístupné nebo bylo určeno ke zveřejnění (např. na základě zákona č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů). Narušení důvěrnosti aktiva neohrožuje oprávněné zájmy XXXXXX. |
| 2 | Střední | Aktivum není veřejně přístupné a tvoří know-how XXXXXX. Ochrana aktiva není vyžadována žádným zvláštním právním předpisem nebo smluvním ujednáním. |
| 3 | Vysoká | Aktivum není veřejně přístupné a jeho ochrana je vyžadována zvláštními právními předpisy, jinými předpisy nebo smluvními ujednáními. |
| 4 | Kritická | Aktivum není veřejně přístupné a vyžaduje nadstandardní míru ochrany nad rámec úrovně „Vysoká“ (např. strategické obchodní tajemství, zvláštní kategorie osobních údajů, apod.). |

Tabulka č. 1 Stupnice pro hodnocení důvěrnosti.

1. Hodnocení integrity je provedeno na stupnici dle Tabulky č. 2:

| **Úroveň** | | **Popis** |
| --- | --- | --- |
| 1 | Nízká | Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy XXXXXX. |
| 2 | Střední | Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů XXXXXX a může se projevit méně závažnými dopady na primární aktiva. |
| 3 | Vysoká | Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů XXXXXX s podstatnými dopady na primární aktiva. |
| 4 | Kritická | Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů XXXXXX s přímými a velmi vážnými dopady na primární aktiva. |

Tabulka č. 2 Stupnice pro hodnocení integrity.

1. Hodnocení dostupnosti je provedeno na stupnici dle Tabulky č. 3:

|  |  |  |
| --- | --- | --- |
| Úroveň | | Popis |
| 1 | Nízká | Narušení dostupnosti aktiva není důležité a v případě výpadku je připuštěno delší časové období pro nápravu (cca do 1 týdne). |
| 2 | Střední | Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne; dlouhodobější výpadek vede k možnému ohrožení XXXXXX. |
| 3 | Vysoká | Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů XXXXXX |
| 4 | Kritická | Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů XXXXXX. |

Tabulka č. 3 Stupnice pro hodnocení dostupnosti.

Informace musí být označovány tak, aby bylo umožněno jejich sdílení a uspořádání. Označování je prováděno dle schématu klasifikace a dle typu média (fyzické označení, metadata).

1. Výsledek hodnocení aktiv je zapsán v evidenci aktiv.

### Evidence primárních aktiv

1. Manažer KB je odpovědný za vedení centrální evidence primárních aktiv v elektronické podobě.
2. Evidence je vedena centrálně pro primární i podpůrná aktiva.
3. Evidence je vedena hierarchicky s příslušnými vzájemnými vazbami.
4. Aktiva mohou být v evidenci seskupována.
5. Minimální rozsah evidovaných informací o aktivu je:
   1. jednoznačný identifikátor,
   2. název,
   3. stručný popis,
   4. typ,
   5. garant,
   6. lokalizace,
   7. hodnocení dostupnosti,
   8. hodnocení integrity,
   9. hodnocení důvěrnosti,
   10. vazba mezi aktivy,
   11. případná navržená opatření.

### Identifikace, hodnocení a evidence podpůrných aktiv

1. Podpůrná aktiva identifikuje Manažer KB ve spolupráci s Garantem primárního aktiva a zaměstnanci, v jejichž gesci je zajištění rozvoje, použití a bezpečnosti primárních a podpůrných aktiv.
2. Součástí identifikace podpůrných aktiv je určení vazby mezi primárními a podpůrnými aktivy.

### Pravidla ochrany jednotlivých úrovní aktiv

1. Ochrana aktiv je odvozena od úrovně hodnocení důvěrnosti, integrity, dostupnosti a citlivosti primárních aktiv. Je stanovena a řízena dokumentací jednotlivých aktiv.
2. Garant aktiva stanoví přípustné způsoby používání primárních aktiv.
3. Dočasné nebo trvalé kopie aktiv (informací nebo dat) včetně médií, na kterých jsou uloženy, musí být chráněny stejným způsobem jako aktiva.
4. Aktiva mohou být používána pouze v souladu s pravidly pro jejich používání definovanými platnou legislativou, bezpečnostní a provozní dokumentací XXXXXX a s ostatní dokumentací (uživatelské a metodické příručky výrobce apod.)
5. Média, uchovávající aktiva, musí být chráněna při přepravě v souladu s klasifikací uložených aktiv.
6. Důvěrnost informací je klasifikována z hlediska významnosti pro XXXXXX, rizika prozrazení nebo modifikace a legislativních požadavků.
   1. Informace s nízkou důvěrností:
      1. jsou veřejně přístupné bez omezení,
      2. nenarušují důvěrnost primárních aktiv a neohrožují zájmy XXXXXX,
      3. v provozní a bezpečnostní dokumentaci IS se označují značkou „Bílá“ nebo „TLP:WHITE“, případně se neoznačují.
   2. Informace se střední důvěrností:
      1. nejsou veřejně přístupné bez omezení,
      2. jsou bez omezení přístupné zaměstnancům XXXXXX,
      3. jsou poskytovány nebo šířeny s definovaným omezením,
      4. jsou přenášeny po veřejných komunikačních sítích jen určeným příjemcům,
      5. v provozní a bezpečnostní dokumentaci IS se označují značkou „Zelená“ nebo „TLP:GREEN“.
   3. Informace s vysokou důvěrností:
      1. nejsou veřejně přístupné,
      2. jsou sdíleny pouze mezi vymezeným oprávněným okruhem příjemců,
      3. jsou sdíleny tak, že je vyhotoven záznam o přístupu nebo přenosu,
      4. jsou přenášeny po veřejných komunikačních sítích jen určeným příjemcům s použitím ochranných kryptografických prostředků,
      5. v provozní a bezpečnostní dokumentaci IS se označují značkou „Oranžová“ nebo „TLP:AMBER“.
   4. Informace s kritickou důvěrností:
      1. nejsou veřejné přístupné,
      2. jsou sdíleny pouze mezi taxativně vymezeným oprávněným okruhem příjemců,
      3. jsou sdíleny tak, že je vyhotoven záznam o přístupu nebo přenosu,
      4. jsou přenášeny po veřejných komunikačních sítích jen určeným příjemcům s použitím ochranných kryptografických prostředků a současně zabraňující zneužití jinými subjekty,
      5. v provozní a bezpečnostní dokumentaci IS se označují značkou „Červená“ nebo „TLP:RED“.

### Způsoby spolehlivého mazání nebo ničení technických nosičů dat a jejich kopií

1. Pro přepravu, mazaní, prodej a likvidaci technických nosičů jsou stanovena závazná provozní pravidla.
2. Likvidace a mazání technických nosičů dat je závislá na typu nosiče a na úrovni důvěrnosti informací na nosiči a provádějí ji pouze určené osoby.
3. Způsob likvidace dat je stanoven přiměřeně k hodnotě aktiva a nákladům na likvidaci média, na kterém jsou data uložena ve smyslu přílohy č.3 Vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.
4. Likvidace informací a dat je prováděna v souladu se Spisovým řádem SM-ORG-12 a zvláštním právním předpisem[[7]](#footnote-7)).

## Politika řízení dodavatelů

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je poskytnout rámec řízení vztahů s dodavateli v souladu se zákonem o kybernetické bezpečnosti[[8]](#footnote-8)).

Při řízení bezpečnosti aktiv XXXXXX jsou rozlišováni následující typy dodavatelů:

|  |  |
| --- | --- |
| Typ dodavatele | Popis |
| Dodavatel | Subjekt, který se podílí na provozu, rozvoji, správě nebo bezpečnosti IS. |
| Významný dodavatel | Provozovatel IS a každý, kdo vstupuje do právního vztahu, který je významný  z hlediska bezpečnosti IS. |

Tabulka č. 4: Základní rozdělení dodavatelů

### Pravidla a principy pro výběr dodavatelů

1. Výběr dodavatelů se řídí zejména zákonem o zadávání veřejných zakázek[[9]](#footnote-9)) a interními akty řízení.
2. Zadávací dokumentace zohledňuje požadavky zákona o kybernetické bezpečnosti. Musí být definován rozsah a úroveň služeb, které budou od dodavatele v rámci veřejné zakázky požadovány.
3. Dodavatelé, kteří mají smluvní vztah s XXXXXX musí být uvedeni v dokumentu, který slouží k jejich evidenci.

### Pravidla pro hodnocení rizik dodavatelů

1. Hodnocení rizik dodavatelů je součástí přípravy zadávací dokumentace veřejné zakázky.
2. Za provedení hodnocení rizik dodavatelů odpovídá zadavatel v součinnosti se správcem IS resp. garantem aktiva.
3. Na základě zjištěné míry rizika přijímají Garanti příslušná bezpečnostní opatření před uzavřením smlouvy nebo v rámci již uzavřených smluvních vztahů.

|  |  |
| --- | --- |
| Rizikový profil dodavatele | Popis rizika |
| A | Nebyly zjištěný žádné informace, které by měly negativní vliv na plnění smluvních povinností nebo na bezpečnost IS. |
| B | Byly zjištěny drobné nedostatky, které mohou být sníženy méně náročnými opatřeními nebo jsou v případě vyšší náročnosti opatření akceptovatelné. |
| C | Byly zjištěny zásadní negativní informace vztahující se k činnosti dodavatele. |

Tabulka č. 5: Úroveň rizika dodavatele

Výsledný rizikový profil dodavatele musí být uveden v dokumentu Evidence dodavatelů. V průběhu smluvního vztahu s dodavateli musí být pravidelně zpravidla jednou ročně prováděno hodnocení rizik souvisejících s dodavateli z důvodu možného dopadu zjištěných informací na plnění zakázky nebo z důvodu možného narušení bezpečnosti aktiv.

### Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.

1. Smlouva s dodavatelem obsahuje popis úrovně služeb (tzv. SLA). Pro konkrétní případ se stanovují takové parametry úrovně služeb, které zohlední povahu plnění smlouvy.
2. Ve smlouvě jsou stanoveny požadavky na:
   1. úroveň služeb,
   2. způsob komunikace pro řízení BU a BI,
   3. způsob a úroveň realizace bezpečnostních opatření,
   4. podmínky výkonu kontrolní činnosti zaměřené na dodržování stanovených bezpečnostních opatření dodavatelem,
   5. povinnost dodavatele realizovat nápravná opatření z kontrolní činnosti,
   6. určení vzájemné smluvní odpovědnosti v oblasti bezpečnosti informací,
   7. výši sankcí za porušení povinností v oblasti bezpečnosti informací,
   8. pravidla náhrady škody,
   9. pravidla pro řízení dokumentace,
   10. pravidla při ukončení smluvního vztahu (tzv. “Exit plan“),
   11. a další v souladu se zvláštním právním předpisem [[10]](#footnote-10)).

### Pravidla pro provádění kontroly zavedení bezpečnostních opatření

1. Potřeba kontroly zavedení a dodržování bezpečnostních opatření dodavatelem je součástí hodnocení rizik dodavatelů.
2. Mezi kontrolní mechanismy patří:
   1. bezpečnostní audit u dodavatele,
   2. výkon plánovaných nebo nahodilých kontrol,
   3. následné kontroly k ověření realizace nápravných opatření,
   4. sledování dodržovaní smluvně stanovené úrovně služeb.
3. Musí být pravidelně prováděna kontrola zavedení bezpečnostních opatření prostřednictvím přezkoumávání plnění smluv v rozsahu dodržování požadavků na bezpečnostní opatření a z hlediska SŘBI. Kontrolu provádí Garant aktiva ve spolupráci s MKB.
4. Musí být minimálně 1x ročně prováděno monitorování a přezkoumávání úrovně poskytovaných služeb dodavatelem.
5. Musí být prováděny audity bezpečnostních opatření a přezkoumávány zprávy auditorů.
6. Pro případy nedodržení některých z bezpečnostních ustanovení ze strany dodavatele musí být ve smlouvě uvedena výše sankce a způsob, jakým budou nahrazeny případné škody.

### Pravidla pro informování významného dodavatele

Musí být vedena evidence významných dodavatelů, která musí být pravidelně aktualizována. Významný dodavatel musí být informován o tom, že se stal významným dodavatelem.

### Pravidla pro hodnocení dodavatelů

1. Hodnocení dodavatelů je prováděno pravidelně a v rámci akceptace plnění.
2. Při hodnocení dodavatele je třeba zohlednit alespoň následující aspekty:
   1. dodržovaní smluvně stanovené úrovně poskytování služeb,
   2. výsledky kontrol,
   3. dodržení smluvních termínů,
   4. vyřizování reklamací,
   5. počet a kvalitu řešení identifikovaných bezpečnostních incidentů (BI) vztahujících se k plnění smlouvy.
3. O výsledku hodnocení dodavatele je informován Manažer KB.
4. Negativní hodnocení dodavatele v oblasti bezpečnosti informací je projednáno výborem.

## Politika bezpečnosti lidských zdrojů

### Předmět

Tato část Politiky organizačních a technických opatření kybernetické bezpečnosti je souhrn zásad a požadavků dopadajících na zaměstnance během celého jeho životního cyklu v organizaci počínaje nástupem, přes jeho výkon, případné změny a konče jeho odchodem. Je navázána na nakládání zaměstnance s aktivy organizace včetně přístupů k aktivům, fungujících na principech definovaných ve směrnici SM-IKT-01 Politika bezpečnosti informací.

Tyto zásady platí i pro externí subjekty, které se podílejí na správě a provozu informačních systémů XXXXXX nebo mají přístup ke kritickým aktivům XXXXXX. Povinnost externích subjektů (dodavatelů) vyžadovat plnění těchto zásad od svých zaměstnanců musí být součástí smluvních ujednání.

Cílem bezpečnosti lidských zdrojů je mimo jiné osvojení znalostí, jak předcházet bezpečnostním událostem a incidentům, jak se chovat v neobvyklých situacích a jak se z nich poučit. To znamená, že zaměstnanci:

* 1. porozumí své roli a budou si vědomi své zodpovědnosti vůči organizaci a okolí;
  2. pochopí zásady systému řízení bezpečnosti informací a z nich vyplývající postupy;
  3. se chovají v souladu se stanovenými bezpečnostními opatřeními;
  4. budou mít znalosti o řídících, provozních a technických mechanismech používaných k zajištění bezpečnosti aktiv, za které odpovídají anebo se kterými pracují.

Pro zajištění dosažení cílů této politiky jsou činěny následující kroky:

1. Školení a závazky na dodržování bezpečnosti informací:
2. všichni zaměstnanci musí být proškoleni první den nástupu do práce a zavázat se mlčenlivostí;
3. třetí strany (dodavatelé apod.) se zavazují k dodržování bezpečnosti informací v rámci uzavřených smluvních vztahů, v případě, že je třetí strana také zpracovatelem osobních údajů, musí mít uzavřenu Zpracovatelskou smlouvu s XXXXXX;
4. bezpečnostní dokumentace SŘBI
   * 1. je řízena, v rámci organizace komunikována, chráněna z pohledu důvěrnosti, integrity a dostupnosti a vedena tak, aby informace v ní obsažené byly úplné a snadno vyhledatelné,
     2. musí být přiměřeně dostupná třetím stranám (v souvislosti s předmětem činnosti);
5. školení jsou prováděna při významných změnách, které mají dopad na systém řízení bezpečnosti informací, nebo podle potřeby;
6. periodická školení jsou prováděna minimálně jednou za rok.
7. Prověřování zaměstnanců a třetích stran v souladu s interními předpisy, aby se minimalizovalo riziko narušení bezpečnosti informací a porušení zásad kybernetické a informační bezpečnosti.
8. Přijímání bezpečnostních opatření na minimalizaci rizik z úmyslného či neúmyslného narušení bezpečnosti informací.

### Organizace řízení bezpečnosti lidských zdrojů

Posuzování uchazečů o zaměstnání je součástí výkonu personálních činnostídle interních předpisů a v souladu s obsahem pracovněprávních vztahů a smluv. Zaměstnanec je z hlediska bezpečnosti sledován po celou dobu trvání pracovněprávního vztahu.

1. Úsek personální, mzdový a vzdělávání v rámci řízení bezpečnosti lidských zdrojů:
2. stanoví s ohledem na stav a potřeby systému řízení bezpečnosti informací plán rozvoje bezpečnostního povědomí, formu, obsah a rozsah školení;
3. určí osoby odpovědné za realizaci uvedených činností;
4. v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o systému řízení bezpečnosti informací organizace formou vstupních a periodických školení;
5. zajistí pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí odborná školení, přičemž vychází z aktuálních potřeb organizace v oblasti kybernetické bezpečnosti;
6. zajistí v souladu s plánem rozvoje bezpečnostního povědomí pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;
7. zajistí v součinnosti s MKB a s příslušnými útvary kontrolu dodržování bezpečnostních politik a pravidel / zásad systému řízení bezpečnosti informací ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;
8. v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role a uživateli zajistí předání odpovědností, navrácení aktiv a zrušení přístupových práv;
9. hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí a
10. určí pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.
11. při provádění školení z oblasti bezpečnosti informací a ochrany osobních údajů spolupracuje s Manažerem kybernetické bezpečnosti a Pověřencem pro ochranu osobních údajů.
12. Oddělení personální a mzdové vede o bezpečnostních školeních přehledy, které obsahují minimálně předmět školení a seznam osob, které školení absolvovaly.
13. Vedoucí zaměstnanci na všech stupních řízení v rozsahu pracovních míst, která zastávají, odpovídají za splnění úkolů zaměstnavatele v oblasti systému řízení bezpečnosti informací a k zajištění bezpečnosti lidských zdrojů.
14. Na revizi a aktualizaci politiky a pravidel týkající se bezpečnosti lidských zdrojů v návaznosti na přezkoumání plánu rozvoje bezpečnostního povědomí a vyhodnocení účinnosti rozvoje bezpečnostního povědomí se podílí minimálně jednou ročně manažer kvality XXXXXX.
15. Musí být vedena evidence docházky zaměstnanců, ze které je patrná jejich přítomnost či nepřítomnost (čerpání dovolené nebo volna, nemoc apod.) na pracovišti. Je důležité pro případné forenzní vyšetřování kybernetického bezpečnostního incidentu.
16. Zaměstnanci musí v průběhu pracovního poměru dodržovat pravidla stanovená v politikách řízení bezpečnosti informací.

### Ukončení a změna pracovního poměru

1. Musí být zajištěno, aby zaměstnanec neprodleně po ukončení pracovního poměru či smlouvy vrátil veškerá svěřená aktiva.
2. Musí být zajištěno, aby zaměstnanec neprodleně po změně pracovního poměru nebo smlouvy vrátil svěřená aktiva, která nejsou dále potřebná pro výkon jeho pracovní role.
3. Řízení přístupů v případě ukončení nebo změně pracovního poměru či smlouvy musí být v souladu s pravidly uvedenými v kapitole č. 12 Politika řízení přístupu.
4. V případě ukončení smluvního vztahu s klíčovými zaměstnanci nebo zaměstnanci zastávajícími bezpečnostní role musí být zajištěno předání odpovědností.
5. Případné odpovědnosti a povinnosti zůstávající v platnosti i po ukončení pracovního poměru musí být obsaženy v pracovní smlouvě zaměstnance nebo ve smlouvě s dodavatelem.
6. Veškerá přístupová oprávnění musí být pravidelně kontrolována v souladu kapitolou č.12 Politika řízení přístupu.

## Politika řízení provozu a komunikací

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je zajistit spolehlivý, stabilní a bezpečný provoz IS a podpůrných aktiv tak, aby byla zaručena bezpečnost primárních aktiv.

### Pravomoci a odpovědnosti spojené s bezpečným provozem

1. Bezpečnostní správce v rámci řízení provozu a komunikací pomocí technických nástrojů pro zaznamenávání činností IS, jejich uživatelů a administrátorů pravidelně vyhodnocuje získané informace a na zjištěné nedostatky reaguje v souladu s postupy zvládání bezpečnostních událostí a incidentů (BU a BI).
2. Bezpečnostní správce v rámci řízení provozu a komunikací zajišťuje bezpečný provoz IS. Za tímto účelem stanoví pravidla a postupy v provozní dokumentaci a bezpečnostní dokumentaci.

### Postupy bezpečného provozu

1. Provozní postupy IS jsou dokumentovány v provozní dokumentaci. Za vedení provozní dokumentace odpovídá příslušný garant aktiva a administrátor.
2. Bezpečnostní postupy IS jsou dokumentovány v bezpečnostní dokumentaci. Za vedení bezpečnostní dokumentace odpovídá příslušný Bezpečnostní správce.
3. Postupy bezpečného provozu zahrnují zejména:
4. práva a povinnosti osob zastávajících role zejména administrátorů a uživatelů,
5. postupy pro spuštění a ukončení chodu IS, pro restart nebo obnovení chodu IS po selhání a pro ošetření chybových stavů nebo mimořádných jevů,
6. postupy pro sledování BU a BI a pro ochranu přístupu k záznamům o těchto činnostech,
7. kontaktní údaje na osoby, které jsou určeny jako podpora při řešení neočekávaných systémových nebo technických problémů,
8. postupy řízení a schvalování provozních změn.
9. Provozní dokumentaci tvoří zejména:
10. provozní deník,
11. plán kontrol řízení provozu,
12. evidence kontrol řízení provozu,
13. zálohovací plán, komunikační matice pro případ vzniku neočekávaných provozních nebo technických problémů,
14. speciální instrukce pro zacházení s výstupy a médii,
15. procedury pro restart a obnovu v případě selhání IS.
16. požadavky a standardy bezpečného provozu

### Řízení změn

1. Veškeré změny v organizaci, provozních procesech, informačních systémech a ve vybavení pro zpracování informací, které mohou mít vliv na bezpečnost informací, musí být dokumentovány.
2. Dokumentace musí obsahovat informace o tom, kdo je oprávněn provádět změny. Změny pak mohou provádět pouze osoby k tomu oprávněné.
3. Musí existovat formální procesy pro řízení změn informačních systémů XXXXXX, které zahrnují:
   * způsob identifikace a zaznamenání významných změn,
   * plánování a testování změn,
   * posouzení možných dopadů těchto změn a ověření, zda byly splněny požadavky na bezpečnost informací,
   * formální postup schvalování navrhovaných změn a seznámení všech příslušných osob s podrobnostmi změn,
   * postupy pro přerušení prováděných změn a obnovení provozu po implementaci neúspěšných změn a při nepředvídaných událostech.

### Řízení kapacit

1. Řízení kapacit je založeno na stanovení kapacitních nároků pro každý IS. Bezpečnostní správce odpovídá za celkové sledování kapacit, předpokládaný vývoj a návrh případných nápravných opatření.
2. Prvky podléhající řízení kapacit jsou:
   * + 1. hardware (výkon, licence)
       2. software (verze, licence),
       3. komunikační infrastruktura (propustnost),
       4. pracovní prostory (prostory pro hardware včetně vybavení, kancelářské prostory),
       5. personální obsazení.

V případě zjištění kapacitního nedostatku musí být tato skutečnost sdělena garantovi systému, případně příslušnému vedení.

### Oddělení prostředí vývoje, testování a provozu

Vývojové a testovací prostředí musí být odděleno od provozního prostředí. V provozním prostředí nesmí být dostupné nástroje pro vývoj, jako jsou například kompilátory. Provozní a projektová dokumentace stanoví, za jakých podmínek dochází k přesunu systému z fáze vývoje a testování do provozního stavu.

### Zaznamenávání událostí

1. Musí být automaticky vytvářeny záznamy událostí obsahující aktivity uživatelů, výjimky a závady v provozu systémů a dále události bezpečnosti informací.
2. Tyto záznamy musí být uchovávány po dobu minimálně 18 měsíců u systémů provozovaných jako kritická informační infrastruktura a po dobu minimálně 12 měsíců u ostatních systémů. Záznamy musí být pravidelně přezkoumávány.
3. Zaznamenané logy musí obsahovat minimálně tyto informace:
   * + - jednoznačnou identifikaci účtu (procesu), pod kterým byla činnost provedena,
       - datum a čas události,
       - identifikaci zařízení (technického aktiva), které činnost zaznamenalo,
       - informace o typu činnosti.
4. Dále musí logy obsahovat tyto informace, jsou-li relevantní pro danou činnost:
   * + - záznamy o úspěšných a odmítnutých pokusech o přístup k systému nebo informacím;
       - změny konfigurace systému,
       - soubory, ke kterým bylo přistupováno,
       - jednoznačnou síťovou identifikaci zařízení, včetně použitých protokolů,
       - úspěšnost nebo neúspěšnost činnosti,
       - záznamy transakcí provedených uživateli.
5. Musí být zamezeno pokusům o neoprávněný přístup k logům, jejich neautorizovanou změnu nebo vymazání.

### Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů

1. Audit KB a bezpečnostní test nesmí omezit provoz a bezpečnost auditovaných IS.
2. Audit KB za účelem ověření provozu IS je naplánován tak, aby se minimalizovalo narušení činnosti auditovaného subjektu.
3. V případě, že Auditor KB potřebuje jiný typ přístupu než pouze pro čtení, vyhotoví provozovatel IS kopie požadovaných souborů a předá je Auditorovi KB. Kopie souborů se po ukončení auditu auditorem smazány nebo, pokud je to vyžadováno Auditorem KB pro dokumentaci auditu, musí být řádným způsobem chráněny.
4. Požadavky, postupy a odpovědnosti Auditora KB jsou dokumentovány.
5. Přístupy Auditora KB jsou monitorovány a logovány.

## Politika řízení změn

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti:

* 1. stanovit způsob a principy řízení změn (včetně významných) z pohledu bezpečnosti informací,
  2. stanovit způsob přezkoumávání dopadů změn,
  3. stanovit způsob vedení evidence a testování změn.

### Způsob a principy řízení změn v procesech a informačních a komunikačních systémech

1. Veškeré změny v rámci prvků ICT, které mají vliv na bezpečnost informací, jsou řízeny, kontrolovány a dokumentovány.
2. Strategické změny jsou součástí strategického řízení a mají delší životní cyklus. Probíhají podle předem naplánovaných, dlouhodobých a schválených záměrů.
3. Rozvojové změny vyvolávají další změny v procesech a zdrojích. Jsou vázány na již existující prvky ICT.
4. Změny jsou realizovány s využitím principů projektového řízení.
5. Změny zahrnují:
   1. změny ovlivňující více uživatelů,
   2. změny prováděné na základě změn platné právní úpravy,
   3. změny dle rozsahu poskytované služby,
   4. změny jednotlivých prvků ICT.

### Přezkoumávání dopadů změn

1. Přezkoumávání dopadů změn je součástí principů projektového řízení.
2. V rámci přezkoumání dopadů změn jsou zohledněny aspekty:
   1. dopadu na funkčnost prvku ICT,
   2. finanční náročnosti změny,
   3. požadavku na personální zdroje pro realizaci změny a pro provozování změněného IS,
   4. dopadu změny na kvalitu poskytovaných služeb (SLA),
   5. dopadu na existující procesy, pracovní postupy a dokumentaci IS,
   6. přidělení rolí a odpovědností při a po realizaci změny,
   7. identifikace a řízení rizik spojených se změnou.
3. Výsledky přezkoumání dopadů změn jsou zohledněny při přípravě plánu realizace změny.
4. Výstupem z přezkoumání dopadů změny je rozhodnutí o realizaci změny.

### Způsob vedení evidence a testování změn

1. Změny jsou dokumentovány.
2. Dokumentace změny obsahuje:
   1. výsledek přezkoumání dopadů změny,
   2. rozhodnutí o realizaci změny,
   3. stanovení osob a jejich odpovědnosti za realizaci změny,
   4. plán nasazení změny,
   5. požadavky na projektovou, provozní a bezpečnostní dokumentaci,
   6. plán testování změny,
   7. akceptaci změny.
3. Plán testování změn obsahuje:
   1. definici rozsahu a druhy testů,
   2. časový harmonogram testování,
   3. rozsah rolí určených pro testování,
   4. školení rolí určených pro testování,
   5. testovací scénáře,
   6. metriky testování,
   7. stanovení způsobu hodnocení testů,
   8. vyhodnocení testů,
   9. akceptaci testů.

Plán testování vytvoří garant aktiva, kterého se změna dotýká ve spolupráci s MKB případně v součinnosti s dodavatelem.

## Politika řízení přístupu

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je:

1. definovat princip a stanovit minimální oprávnění,
2. definovat požadavky na nastavení přístupových práv pro uživatele, privilegované uživatele a bezpečnostní role včetně souvisejících procesů,
3. stanovit fáze řízení přístupových práv,
4. definovat základní požadavky na technologické účty,
5. specifikovat základní principy pro privilegovaná oprávnění a omezení při jejich užití,
6. specifikovat proces pro přidělování, správu a rušení přístupových práv v případě mimořádných situací,
7. určit způsob a četnost kontrol přístupových práv.

### Pravidla a požadavky na řízení přístupu

1. Za řízení přístupu a stanovení pravidel je odpovědný garant příslušného aktiva.
2. Za stanovení pravidel v oblasti řízení přístupu je odpovědný bezpečnostní správce.
3. Musí existovat evidence všech uživatelských účtů, pomocí které je možné jednoznačně identifikovat osobu používající daný uživatelský účet.
4. Přístupy a pokusy o přístup musí být automaticky zaznamenávány a monitorovány. Záznamy musí být uchovány po dobu minimálně 18 měsíců u systémů provozovaných jako kritická informační infrastruktura a po dobu minimálně 12 měsíců u ostatních systémů. U uživatelských účtů musí být nastaveno automatické uzamčení obrazovky při nepřítomnosti uživatele. Pro opětovné odemčení musí být vyžadovány autentizační údaje.
5. Autentizační údaje nesmí být sdíleny více osobami.
6. Přidělování přístupových práv se řídí pravidly:
7. každý prvek ICT má řízený a dokumentovaný proces přidělování přístupových práv,
8. je prováděna pravidelná kontrola řízení přístupových práv a stanovených pravidel pro řízení přístupových práv,
9. přidělování přístupových práv uživatelům je prováděno pouze v rozsahu nutném pro výkon jejich služebních, resp. pracovních povinností,
10. kontrola přidělených přístupových práv je prováděna při každé změně a minimálně jednou za rok,
11. pro každý prvek ICT je vedena aktuální evidence všech uživatelských účtů,
12. pro každý prvek ICT je definován systém uživatelských rolí a oprávnění,
13. je vedena evidence o uskutečněných přístupech a o pokusech o přístup k aktivu,
14. primárním nástrojem pro řízení uživatelů je nástroj Identity management (IDM)
15. zákaz přístupu k aktivům prostřednictvím veřejných sítí např. z nechráněné sítě v restauracích apod.,
16. je využívána vícefaktorová autentizace,
17. role uživatelů, privilegovaných uživatelů a bezpečnostních rolí jsou odděleny,
18. postup řízení přístupů při mimořádných situacích je dokumentován.

### Princip minimálních oprávnění a potřeby znát (need to know)

Pravidla pro řízení přístupových oprávnění:

1. Každý uživatel má přístup pouze k těm aktivům, která nezbytně potřebuje k výkonu práce.
2. Základní rozsah oprávnění k jednotlivým aktivům je definován jako minimum potřebného pro činnosti, které uživatel potřebuje. Oprávnění jsou členěna do uživatelských rolí.
3. Změna rozsahu přístupových oprávnění je řízena a schvalována.

### Minimální požadavky na systém řízení přístupu

Systém řízení přístupu je tvořen minimálně:

1. popisem rozsahu jednotlivých uživatelských rolí,
2. popisem požadavku na školení jednotlivých uživatelských rolí,
3. definicí kritické kombinace rolí,
4. popisem procesu přidělování uživatelských rolí,
5. popisem technologie ověření identity uživatelů,
6. popisem bezpečného chování uživatelů,
7. definicí životního cyklu přístupových údajů uživatelů,
8. vynucováním pravidel pro ověření identity uživatelů.

### Životní cyklus řízení přístupu

1. Řízení přístupu je dokumentováno pro každé aktivum a probíhá ve fázích:
   1. žádost o přidělení přístupových práv,
   2. schvalování a přidělení přístupových práv,
   3. pravidelná kontrola přístupových práv,
   4. změna přístupových práv,
   5. zrušení přístupových práv.
2. V žádosti o přidělení přístupových práv jsou definovány minimálně:
   1. osoba oprávněna žádat,
   2. uživatel,
   3. rozsah oprávnění a jejich zdůvodnění,
   4. doba platnosti oprávnění.
3. V procesu schvalování a přidělení přístupových práv je definován minimálně:
   1. osoby oprávněné schválit požadavek,
   2. schvalovací lhůty,
   3. osoby nastavující příslušná oprávnění.
4. V procesu změny přístupových práv je definována minimálně:
   1. osoba oprávněna žádat,
   2. uživatel,
   3. požadavek na změnu rozsahu oprávnění,
   4. doba platnosti oprávnění,
   5. osoby oprávněné schválit požadavek,
   6. schvalovací lhůty,
   7. osoby nastavující příslušná oprávnění.
5. Ke zrušení přístupových práv k informacím a aktivům dochází:
   1. při ukončení nebo změně pracovního nebo smluvního vztahu nebo výkonu role uživatele,
   2. na základě procesů definovaných v provozní dokumentaci jednotlivého aktiva.

### Řízení privilegovaných oprávnění

1. Privilegovaným oprávněním se rozumí přístupové oprávnění k účtu, které umožnuje v jednotlivém prvku ICT:
   1. vykonávat činnosti nad rámec běžného uživatele IS,
   2. provádět změny v nastavení IS,
   3. měnit rozsah přidělených oprávnění jednotlivých rolí a uživatelů,
   4. vykonávat servisní činnosti bez přítomnosti uživatele.
2. Pro privilegované oprávnění je přiřazen odlišný identifikátor uživatele od běžně používaného uživatelského účtu.
3. Běžné činnosti nesmějí být prováděny s použitím privilegovaného oprávnění.
4. Musí být nastaveno časové omezení platnosti přihlašovací relace, po jehož vypršení následuje automatické odhlášení od systému.

### Řízení přístupu pro mimořádné situace

1. Za účelem zajištění kontinuity činnosti během BU, BI nebo jiných mimořádných situací jsou jednorázově nastavena přístupová oprávnění nad rámec standartního režimu provozu prvku ICT.
2. Procesy pro zvládání BU, BI nebo jiné mimořádné situace jsou definovány v havarijním plánu a zpracované pro všechna relevantní informační aktiva.

### Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách

1. Proces pro přezkum přístupových oprávnění je definován v bezpečnostní dokumentaci zpracované pro každé aktivum.
2. Kontrola přístupových oprávnění v jednom cyklu je provedena na celém rozsahu uživatelských oprávnění.
3. Dokumentace pro přezkum přístupových oprávnění obsahuje minimálně:
   1. stanovení cyklu provádění kontroly,
   2. osoby provádějící kontrolu,
   3. zápis o provedené kontrole,
   4. postup nápravy při zjištění nedostatku.

## Politika bezpečného chování uživatelů

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je:

* 1. definovat zásady bezpečného chování uživatelů,
  2. stanovit povinnosti uživatelů,
  3. definovat pravidla bezpečného provozu IS.

### Pravidla pro bezpečné nakládání s aktivy

1. Pravidla pro zacházení s aktivy jsou stanovena na základě zejména jejich klasifikace a jsou dokumentována pro každé aktivum (zejména technické).
2. Uchovávání, ukládání a archivace informací, dat a procesů je prováděno tak, aby byla zajištěna jejich dostatečná ochrana před neoprávněným přístupem a aby bylo znemožněno jejich jiné zneužití.
3. Každý uživatel má přístup pouze k těm aktivům, která nezbytně potřebuje k výkonu své pracovní náplně.
4. Případné výjimky z pravidel jsou realizovány na základě odůvodněné a schválené žádosti. Žádost schválí přímý nadřízený žadatele a postoupí ji manažerovi kybernetické bezpečnosti, který ji schválí nebo zamítne a postoupí ji vedoucímu Odboru informatiky k technické realizaci.

### Bezpečné použití přístupového hesla

1. Každý prvek ICT má v bezpečnostní dokumentaci k aktivu stanovena pravidla pro vytváření a používání hesel, která jsou vymáhána systémovými prostředky pro různé typy oprávnění.
2. Uživatelé musí uchovávat a používat hesla takovým způsobem, aby nebyly vyzrazeny jiným osobám.
3. Uživatelé musí používat rozdílná hesla pro systémy XXXXXX a pro služby, aplikace a systémy používané pro soukromé účely.
4. Uživatelé jsou o aktuálních parametrech jednotlivých pravidel tvorby silného hesla informování při registraci, případně při změně hesla.
5. Pravidla tvorby hesel stanovují minimálně tyto parametry:
6. minimální délka hesla,
7. použití kombinace malých, velkých písmen, číslic a speciálních znaků,
8. možnost vyžádané změny hesla,
9. povinná změna hesla po určité době,
10. zákaz tvorby hesla ze skutečnosti, kterou může někdo snadno odhadnout nebo ji získat z osobních informací, např. jméno, telefonní číslo, datum narození apod., nenapadnutelnost slovníkovým útokem (tj. neskládají se ze slov obsažených ve slovníku), zákaz shody s přihlašovacím jménem,
11. nemožnost použít opakovaně stejné heslo při jeho změně,
12. povinná bezodkladná změna výchozího hesla po prvním použití,
13. povinné bezodkladné zneplatnění hesla sloužícího k obnovení přístupu po jeho prvním použití nebo uplynutím definované doby od jeho vytvoření atd.

### Bezpečné použití elektronické pošty a přístupu na internet

1. V rámci elektronické pošty jsou nastavena následující pravidla:
   1. informace obsažené v elektronicky předávaných zprávách je nutno přiměřeně chránit,
   2. uživatelé mohou používat elektronickou poštu pouze k plnění pracovních úkolů,
   3. u informací s vysokou úrovní důvěrnosti jsou vyžadovány kryptografické prostředky pro jejich ochranu.
2. Při použití elektronické pošty je zakázáno:
   1. otevírat přílohy zpráv z jiných než důvěryhodných zdrojů,
   2. používat prostředky elektronické pošty XXXXXX pro soukromé účely,
   3. používat pro pracovní komunikaci veřejné e-mailové služby (např. Gmail, Seznam apod.),
   4. otevírat přílohy a webové odkazy z e-mailů od neznámých zdrojů. V případě výskytu podezřelého e-mailu je uživatel povinen nahlásit tuto skutečnost MKB nebo na odbor informatiky,
   5. nastavovat pravidla pro automatické přeposílání elektronické pošty mimo XXXXXX.
3. V rámci přístupu na internet jsou nastavena následující pravidla:
   1. používat služeb internetu je zakázáno pro jiné než. pracovní účely,
   2. je zakázáno ukládat aktiva XXXXXX na neschválená veřejná úložiště (např. Google drive, One drive, DropBox apod.)
   3. stahovat spustitelné soubory a soubory obsahující makra je zakázáno.

### Bezpečný vzdálený přístup

Bezpečný vzdálený přístup do vnitřních sítí je dokumentovaný a řídí se těmito pravidly:

* 1. je povolen pouze na základě žádosti, předané vedoucímu Úseku informačních technologií a schválené manažerem kybernetické bezpečnosti
  2. pro využívání aktiv XXXXXX prostřednictvím vzdáleného přístupu platí stejná pravidla uvedená v politikách řízení informační bezpečnosti, jako pro práci na pracovišti,
  3. pro vzdálený přístup k aktivům XXXXXX musí uživatelé využít schválené technologie,
  4. vytvořené spojení v rámci vzdáleného přístupu je šifrované a předchází mu dvoufaktorová autentizace uživatele,
  5. přístupy jsou jednoznačně zaznamenány spolu s identifikací uživatele,
  6. uživatelé nesmí sdílet své oprávnění vzdáleného přístupu.

### Bezpečné chování na sociálních sítích

1. Je zakázáno přistupovat pro soukromé účely na účty sociálních sítí v pracovní době a ze zařízení, která jsou ve správě XXXXXX.
2. Je zakázáno zveřejňovat na sociálních sítích neveřejné informace a dokumenty týkající se pracovní náplně a činnosti XXXXXX.
3. Je zakázáno zveřejňovat na sociálních sítích fotografie z interiéru budov XXXXXX.
4. Odstavce 2 a 3 se netýkají oficiálních účtů XXXXXX na sociálních sítí.

### Sdílení informací s vysokou úrovní důvěrnosti

1. Pro jejich sdílení bude stanoveno technické řešení, které zajistí vysokou míru bezpečnosti

### Bezpečnost ve vztahu k mobilním zařízením

1. Mobilními zařízeními se rozumí veškerá mobilní zařízení umožňující zobrazovat, editovat, ukládat, přenášet nebo tisknout data, tedy zejména:
   1. notebooky,
   2. tablety a podobná přenosná zařízení,
   3. chytré telefony,

Každé mobilní zařízení musí být jednoznačně identifikovatelné (např. pomocí MAC adresy, identifikačního nebo sériového čísla).

1. Uživatel je povinen pro pracovní účely používat mobilní zařízení, která mu byla přidělena XXXXXX, nebo která splňují bezpečnostní požadavky XXXXXX.
2. Bezpečnost ve vztahu k mobilním zařízením přiděleným XXXXXX se řídí pravidly:
   1. provádění vlastní modifikace a instalace aplikací na mobilním zařízení je zakázáno,
   2. veškeré instalace aplikací musí být prováděny pouze oprávněným pracovníkem Úseku IT,
   3. uživatel je povinen chránit mobilní zařízení před krádeží a zneužitím,
   4. uživatel je povinen bezodkladně hlásit ztrátu mobilního zařízení,
   5. uživatel nesmí umožnit přístup do mobilního zařízení jiné osobě,
   6. uživatel je povinen ve stanovených intervalech připojit mobilní zařízení do sítě XXXXXX za účelem provedení aktualizací a kontrol,
   7. uživatel nesmí měnit nastavená bezpečnostní pravidla na zařízení,
   8. výměnné disky a paměťové karty, flash paměti musí být šifrovány určeným nástrojem
   9. uživatel je povinen chránit přístup do zařízení heslem, PINem, gestem nebo biometrickým prvkem.
3. Bezpečnost ve vztahu k mobilním zařízením, která XXXXXX nemá ve své správě, se řídí pravidly:
   1. instalace aplikací na mobilním zařízení nesmí ohrozit informace XXXXXX,
   2. uživatel je povinen chránit mobilní zařízení před krádeží a zneužitím,
   3. uživatel je povinen bezodkladně hlásit ztrátu mobilního zařízení obsahující informace XXXXXX,
   4. tato zařízení nesmí být připojena do interní sítě XXXXXX, tato zařízení smí být připojena pouze do izolované bezdrátové sítě XXXXXX\_HOST,
   5. uživatel nesmí umožnit přístup k informacím XXXXXX v mobilním zařízení jiné osobě,
   6. uživatel je povinen používat odpovídající bezpečnostní pravidla na zařízení,
   7. uživatel je povinen chránit přístup do zařízení heslem, PINem, gestem nebo biometrickým prvkem.

## Politika zálohování a obnovy a dlouhodobého ukládání

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je stanovit principy a procesy zálohování dat i zálohování prostředků pro zpracování informací v IS.

### Požadavky na zálohování a obnovu

1. Bezpečnostní správce stanoví požadavky na zálohování pro každé informační aktivum na základě vydefinovaných požadavků na SLA garantem primárních aktiv. Minimální požadavky na zálohování a obnovu jsou:
2. rozsah zálohování,
3. Doba obnovy chodu (Recovery Time Objective – RTO) se rozumí doba, kdy předmětná informační aktiva dosáhnou stanovené úrovně poskytovaných služeb,
4. Bod obnovy dat (Recovery Point Objective – RPO) se rozumí okamžik, ke kterému jsou zpětně obnovena data.
5. Požadavky na zálohování realizuje Bezpečnostní správce minimálně v těchto oblastech:
6. příprava Plánu zálohování,
7. řízení kapacit pro zálohování,
8. provádění záloh a obnovy a aktualizace Plánu zálohování,
9. kontrola záloh,
10. test obnovy.

### Pravidla a postupy zálohování

1. Každý prvek ICT má zpracován Plán zálohování, který obsahuje minimálně:
2. rozsah zálohování,
3. stanovení RTO a RPO,
4. předpokládaný objem zálohovaných dat,
5. určení způsobu zálohy,
6. dobu uchování (retence) záloh,
7. popis tvorby záloh,
8. určení záložního média a způsobu ukládání,
9. zabezpečení záloh a medií,
10. stanovení způsobu a rozsahu testů obnovy ze záloh.
11. Proces zálohování je monitorován. Bezpečnostní správce zodpovídá za úspěšnost procesu zálohování.
12. Data musí být uchovávána v souladu s platnou legislativou určující například dobu jejich uchování, případně, pokud se jedná o osobní údaje, způsoby nakládání s nimi (skartace).

### Pravidla a postupy dlouhodobého ukládání

1. Zálohy pro dlouhodobé ukládání nejsou ukládány na zařízení zálohovaného IS.
2. Zálohy pro dlouhodobé ukládání jsou ukládány mimo lokalitu primárního úložiště dat.
3. Nosiče záloh jsou označeny a evidovány.
4. Úložiště dlouhodobých záloh splňují pravidla fyzické bezpečnosti.
5. Vstup osob do prostor se zálohami je řízen a omezen pouze na oprávněné osoby.

### Pravidla bezpečného zálohování a dlouhodobého ukládání informací

1. Dlouhodobé ukládání je řešeno dle požadavků Garantů primárních aktiv minimálně v rozsahu:
2. doba ukládání informací včetně archivace,
3. způsob přístupu k archivovaným datům,
4. způsob likvidace dat.
5. Dlouhodobé ukládání informací a zálohovacích médií zabezpečuje Bezpečnostní správce na základě požadavků Garanta primárního aktiva.
6. Pravidla bezpečného zálohování a dlouhodobého ukládání informací jsou stanovena v Plánu zálohování.

### Pravidla a postupy obnovy

1. Postupy obnovy obsahují popis procesu obnovy a jsou součástí Plánu zálohování.
2. Pravidla obnovy obsahují minimálně:
3. rozsah obnovy,
4. zdroj obnovy,
5. cíl obnovy,
6. test obnovy.

### Pravidla a postupy testování zálohování a obnovy

1. Kontrola čitelnosti, úplnosti a obnovy dat ze záloh je součástí Plánu zálohování a probíhá pravidelně dle Plánu zálohování.
2. Provedení testů obnovy dat ze zálohy je dokumentováno.
3. Provedením testů obnovy dat nelze narušit provoz žádného prvku ICT.

### V případě zjištění chyb při testu je nutno přijmout opatření k nápravě.

Přístup k zálohám a ukládaným informacím

K zálohovacím médiím mají přístup pouze osoby provádějící zálohování. Ostatní osoby mohou v případě odůvodněné potřeby získat přístup k zálohám na základě povolení MKB.

## Politika bezpečného předávání a výměny informací

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je stanovit pravidla a způsob ochrany pro předávání informací.

### Pravidla a postupy pro ochranu předávaných informací

1. K ochraně přenosu informací prostřednictvím všech druhů komunikačních zařízení jsou stanoveny postupy a opatření na základě klasifikace informací.
2. Dochází-li k předávání informací s externím subjektem (např. smluvní strana), podrobnosti o bezpečném předávání informací jsou definovány dohodou o předávání informací.
3. Dohoda o předávání informací obsahuje zejména:
4. rozsah předávaných informací,
5. způsob zabezpečení předávaných informací, včetně ochrany důvěrnosti, integrity, autentičnosti,
6. účel užití předávaných informací,
7. technické parametry předávaných informací,
8. odpovědnosti a povinnosti v případě vzniku BU a BI,
9. dohodu o mlčenlivosti.
10. Za uzavření dohody o předávání informací odpovídá Garant příslušného aktiva, jehož aktivum je se smluvní stranou sdíleno.
11. Pro předávání informací je zakázáno využívat veřejná internetová úložiště (např. Google drive, One drive, DropBox apod.).
12. Uveřejňování informací na internetových stránkách XXXXXX je řízeno.

### Pravidla pro využívání kryptografické ochrany

1. Kryptografická opatření jsou používána v případech nutnosti zajistit důvěrnost, integritu a autentičnost přenášených informací v souladu s klasifikací aktiv podle článku 8 „ Politika řízení aktiv“
2. Používání prostředků kryptografické ochrany se řídí podle článku 24 „Politika bezpečného používání kryptografické ochrany“

## Politika řízení technických zranitelností

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je:

1. identifikovat zranitelnosti, které by mohly omezit funkčnost nebo bezpečnost provozu prvků ICT,
2. stanovit způsob přijetí opatření k řešení a eliminaci zranitelností,
3. stanovit pravidla pro omezení instalace programového vybavení,
4. stanovit pravidla a postupy vyhledávání opravných programových balíčků,
5. stanovit pravidla a postupy testování oprav programového vybavení,
6. stanovit pravidla a postupy nasazení oprav programového vybavení.

Pro všechny provozované a spravované systémy musí být vypracována metodika nasazení technických zranitelností (patch management), v které je uveden zdroj oprav, plán nasazení, a způsob testování a nasazení

### Technické zranitelnosti ICT produktů

1. Technické zranitelnosti ICT produktů se dělí na:
2. chyby v programovém kódu, které vznikly během vývoje produktů nebo při jejich aktualizacích a opravách,
3. chyby v instalaci a konfiguraci technických prostředků a instalovaného programového vybavení.
4. Proces řízení technických zranitelností prvků ICT je dokumentovaný a je založen na:
5. identifikaci zranitelností,
6. stanovení priorit řešení zranitelností,
7. řešení zranitelností dle priorit,
8. implementace náhradního opatření, není-li oprava dostupná,
9. kontrole aplikovaných opatření.

Nasazení oprav zranitelností musí probíhat v souladu s pravidly pro řízení změn, popsanými v kapitole 11 „Politika řízení změn“.

### Pravidla pro omezení instalace programového vybavení

1. XXXXXX vede evidenci podpůrných aktiv.
2. U programového vybavení evidence obsahuje alespoň následující informace:
   1. dodavatele a výrobce programového vybavení,
   2. aktuální nasazenou verzi,
   3. umístění programového vybavení.
3. Je zakázáno instalovat neschválené programové vybavení, smí být instalováno pouze programové vybavení nezbytné pro správnou funkcionalitu a pro jeho správu.
4. Instalace nového programového vybavení podléhá procesu řízení změn.
5. Garant příslušného aktiva je odpovědný za provedení řádné instalace programového vybavení.

### Pravidla a postupy vyhledávání opravných programových balíčků

1. Bezpečnostní správce v součinnosti s Garantem podpůrného aktiva pravidelně monitoruje informace o technických zranitelnostech z dostupných zdrojů, identifikuje rizika a navrhuje Architektovi KB metody řešení.
2. Architekt KB spolu s příslušnými Garanty aktiv posuzují rizika a stanovují postup řešení.
3. Po odsouhlasení Architektem KB Garant podpůrného aktiva zajistí instalaci opravných programových balíčků.

### Pravidla a postupy testování oprav programového vybavení

1. Testování oprav a nového programového vybavení je realizováno v prostředí odděleném od produkčního prostředí.
2. Testy musí prokázat správnost úprav programového vybavení.
3. Nasazení do produkčního prostředí je realizováno po úspěšném vyhodnocení testů a schválením garantem příslušného aktiva
4. Pokud není možné realizovat testování programového vybavení z důvodu zvýšených nákladů nebo nedostatku zdrojů, je nutno identifikovat a vyhodnotit všechna související rizika nasazení oprav programového vybavení.

### Pravidla a postupy nasazení oprav programového vybavení

1. Pro každý prvek ICT je řízen a dokumentován proces nasazení oprav programového vybavení.
2. V rámci nasazení oprav programového vybavení do produkčního prostředí jsou vytvořeny body návratu (RPO) a zálohy dat.
3. V případě nasazení oprav programového vybavení jsou zálohovány předchozí verze programového vybavení.

## Politika řízení kontinuity činností

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je:

1. stanovit práva a povinnosti zúčastněných osob,
2. stanovit cíle řízení kontinuity činností s ohledem na minimální úroveň poskytovaných služeb, dobu obnovení chodu IS a bodu obnovení dat,
3. stanovit způsoby hodnocení dopadů BI na kontinuitu a posuzování souvisejících rizik,
4. určit obsah plánů kontinuity činností a havarijních plánů jednotlivých IS.

### Cíle řízení kontinuity činností

1. Cílem řízení kontinuity činností je:
   1. stanovit na základě výstupů hodnocení rizik a analýzy dopadů minimální rozsah poskytovaných služeb jednotlivých agend XXXXXX,
   2. zajistit bezpečnost a kontinuitu poskytování služeb ICT i v podmínkách vzniku BI, BU, mimořádné události nebo v případě narušení poskytování služeb ICT,
   3. zahájit kroky směřující k zajištění obnovy služeb na požadovanou úroveň,
   4. minimalizovat škody na majetku nebo aktivech XXXXXX, vzniklé v důsledku mimořádné události.
2. Procesy kontinuity činností jsou řízeny a dokumentovány.
3. Každý prvek ICT má stanovenu dobu obnovení chodu (RTO) a bod obnovení dat (RPO).
4. Minimální úrovní poskytovaných služeb se rozumí minimální rozsah služeb prvků ICT pro užívání, provoz a správu IS.
5. Dobou obnovení chodu se rozumí doba, kdy prvky ICT dosáhnou stanovené úrovně poskytovaných služeb.
6. Bodem obnovení dat se rozumí okamžik, ke kterému jsou zpětně obnovena data na příslušnou úroveň poskytovaných služeb.
7. Bodem plného obnovení dat se rozumí okamžik, ke kterému jsou plně obnovena data.

### Naplnění cílů kontinuity činností

1. Pro naplnění cílů kontinuity jsou Bezpečnostními správci vypracovány, řízeny a pravidelně aktualizovány plány kontinuity činností a havarijní plány prvků ICT a souvisejících služeb.
2. Plány kontinuity činností a havarijní plány jsou pravidelně testovány.

### Způsoby hodnocení dopadů bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik

Hodnocení dopadů BI na kontinuitu a posuzování souvisejících rizik je součástí analýzy dopadů v rámci hodnocení primárních aktiv a jejich vazeb na podpůrná aktiva. Při stanovení hodnoty aktiv a navazujících rizik je nutno brát v úvahu i dopad na zajištění kontinuity činností daného aktiva.

### Určení a obsah potřebných plánů kontinuity činností a havarijních plánů

1. Plán kontinuity činností a havarijní plán jsou pro IS zahrnuty ve společném dokumentu nazvaném Havarijní plán IS (někdy také plán kontinuity činnosti IS).
2. Havarijní plán IS obsahuje zejména:
   1. hodnotu aktiv a stanovení dopadů a rizik souvisejících s ohrožením kontinuity činností,
   2. minimální úroveň poskytovaných služeb,
   3. dobu obnovení chodu na minimální úroveň poskytovaných služeb,
   4. bod obnovení dat na dosažení minimální úrovně poskytovaných služeb,
   5. dobu obnovení chodu na plnou úroveň poskytovaných služeb,
   6. bod obnovení dat na dosažení plné úrovně poskytovaných služeb,
   7. popis vazeb mezi jednotlivými prvky ICT,
   8. finanční, technické, lidské a informační zdroje nutné pro realizaci,
   9. pravidla pro aktualizaci a plány testování,
   10. opatření použitá k zabránění vzniku BU a BI,
   11. postupy v případě výskytu BU a BI a mimořádné události,
   12. odpovědnosti jednotlivých zúčastněných osob,
   13. časové posloupnosti činností,
   14. návaznosti na havarijní plány jiných IS.

## Politika zvládání kybernetických bezpečnostních incidentů

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je stanovit postupy vedoucí ke snížení dopadů bezpečnostních událostí (BU) a bezpečnostních incidentů (BI) a k zastavení jejich šíření a k prevenci před jejich opakováním.

### Definování kategorií kybernetického bezpečnostního incidentu

1. Kategorie BI jsou stanoveny zvláštním právním předpisem[[11]](#footnote-11)).
2. Kategorie BI je dána úrovní jejich závažnosti a předpokládaného dopadu na aktiva XXXXXX:
   1. kategorie I – méně závažný incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy garantů aktiv nebo administrátorů k omezení dalšího šíření incidentu včetně minimalizace vzniklých škod,
   2. kategorie II – závažný incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy garantů aktiv nebo administrátorů k zabránění dalšího šíření incidentu včetně minimalizace vzniklých škod,
   3. kategorie III – velmi závažný incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy garantů aktiv nebo administrátorů k zabránění dalšího šíření incidentu včetně minimalizace vzniklých i potenciálních škod.

### Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů

1. V XXXXXX je zaveden nástroj pro detekci BU a BI.
2. V XXXXXX je určen nástroj pro evidenci, správu a řešení provozních a bezpečnostních událostí a incidentů, který je jednotným kontaktním místem.
3. Ve XXXXXX jsou stanoveny postupy a role pro analýzu BU, jejich kategorizaci a posouzení, zda se jedná o BI.
4. Postupy zvládání BU a BI jsou stanoveny v závislosti na hodnocení aktiv a rizik jednotlivých prvků ICT.
5. V rámci klasifikace BU a BI jsou posuzovány dopady, nutnost reakce a naléhavost řešení.
6. Forma a náležitosti hlášení BI NÚKIB jsou stanoveny zvláštním právním předpisem1).
7. Za nahlášení BI NÚKIB je ve XXXXXX odpovědný Manažer KB.

### Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů

1. Testování systému zvládání BU a BI je dokumentováno a řízeno.
2. Testování systému zvládání BU a BI je prováděno jednou za rok.
3. K testování systému zvládání BU a BI jsou použita pouze testovací data.

### Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti

1. Každý BI je hodnocen z hlediska dopadů na důvěrnost, dostupnost a integritu jednotlivých aktiv.
2. Výsledky hodnocení BI jsou podnětem pro zlepšování kybernetické bezpečnosti.
3. Opatření plynoucí z vyhodnocení BI jsou podnětem pro aktualizaci Plánu zvládání rizik.
4. Každý BI, jeho vyhodnocení včetně návrhu na opatření jsou předkládána k projednání Výboru.

### Evidence incidentů

1. Evidence BU a BI je ve XXXXXX centrálně vedena v nástroji pro evidenci, správu a řešení provozních a bezpečnostních událostí a incidentů.
2. Za vedení evidence BU a BI je odpovědný Manažer KB.

## Politika akvizice, vývoje a údržby

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je:

* 1. zajistit bezpečnost informací při akvizici, vývoji a údržbě IS a prvků ICT,
  2. stanovit pravidla a postupy při akvizici, vývoji a údržbě programového vybavení včetně jeho evidence,
  3. stanovit pravidla a postupy pro kontrolu dodržování licenčních podmínek.

### Bezpečnostní požadavky pro akvizici, vývoj a údržbu

1. Požadavky na bezpečnost musí být zahrnuty již ve fázi výběru a návrhu systému, musí být zdokumentovány a uvedeny ve smlouvách s dodavateli.
2. Požadavky na bezpečnostní opatření musí být definovány a implementovány na základě klasifikace primárních aktiv daného systému a na základě provedené analýzy rizik.
3. Musí být vytvořena akceptační kritéria zahrnující funkční a bezpečnostní požadavky pro nový systém. Tato kritéria musí být vyhodnocena v rámci akvizice a před uvedením systému do provozu.
4. Při vývoji musí být zajištěna bezpečnost vývojového a testovacího prostředí a jejich oddělení od produkčního prostředí.
5. Přechod nového systému do produkčního prostředí a údržba všech systémů musí být prováděny dle pravidel pro řízení změn uvedených v kapitole 11 „Politika řízení změn“.
6. Po celý životní cyklus systému musí být zajištěno řízení verzí programového vybavení včetně možnosti návratu na předchozí verzi.
7. Provozní, projektová, uživatelská a bezpečnostní dokumentace musí být udržována aktuální po celou dobu vývoje systému.
8. Proces akvizice a vývoje je plánován, dokumentován a řízen.
9. Garant aktiv:
   1. definuje funkční požadavky na akvizici a vývoj jednotlivých prvků ICT,
   2. zajišťuje klasifikaci aktiva,
   3. stanovuje pravidla přístupu k aktivu.
10. Architekt KB navrhuje implementaci bezpečnostních opatření prvků ICT alespoň na úrovni:
    1. bezpečnosti vývojového prostředí,
    2. metodologie vývoje software,
    3. kontrolních bodů bezpečnosti v projektu,
    4. bezpečného úložiště,
    5. řízení verzí,
    6. identifikace zranitelností a návrhu opatření.
11. Garant podpůrných aktiv ve spolupráci s odborem informatiky definuje požadavky na údržbu prvku ICT.
12. Životní cyklus aktiva a proces akvizice obsahuje bezpečnostní požadavky a bezpečnostní opatření v závislosti na platné bezpečnostní politice, identifikovaných rizicích a požadavcích garantů aktiv.
13. Vývoj, změny a údržba aktiv jsou prováděny v souladu se stanoveným procesem, který zohledňuje zásady bezpečného vývoje a řízení změn, testování v rámci odděleného prostředí, kontrolu vytvořeného kódu, případně nezávislou kontrolu bezpečnosti třetí stranou.

### Řízení zranitelností

V rámci akvizice systému a po implementaci významných změn musí být na základě provedené analýzy rizik rozhodnuto o provedení testů zranitelností nebo penetračních testů.

1. Proces řízení zranitelností aktiv je plánován, dokumentován a řízen. Je založen na:
   1. identifikaci zranitelností,
   2. řešení zranitelností dle priorit,
   3. kontrole aplikovaných opatření.
2. Technické přezkoumání aplikací po změnách provozní platformy jednotlivých prvků ICT vyžaduje alespoň:
   1. přezkoumání postupů řízení a integrity aplikací a zabezpečení dat k zajištění, že nebyly změnami provozních platforem kompromitovány,
   2. zajištění včasného oznámení změn provozních platforem, aby bylo před implementací umožněno provedení příslušných testů a přezkoumání,
   3. zajištění provedení příslušných změn v plánech kontinuity činností.
3. Změny programového vybavení jsou omezeny na nezbytné změny a všechny jsou řízeny. V případě, že je nutno programové vybavení upravit, jsou posuzovány následující body:
   1. rizika navrhovaných opatření a procesů zajišťujících integritu,
   2. dodržení licenční politiky,
   3. součinnost s dodavatelem při aktualizaci programového vybavení,
   4. kompatibilita s dalším používaným programovým vybavením.

### Poskytování a nabývání licencí programového vybavení a informací

Na všech zařízeních provozovaných v XXXXXX musí být instalován pouze autorizované programové vybavení s platnou licencí, případně autorizované programové vybavení, pro které zakoupení licence není vyžadováno autorem/dodavatelem.

Doklady a důkazy o právu užití licencí a předplacených službách musí být uchovány v souladu s pravidly stanovenými v článku 8 „Politika řízení aktiv“

1. Pravidla a postupy nasazení programového vybavení a jeho evidence:
   1. Bezpečnostní správce vede evidenci programového vybavení v souladu s obecně platnými právními předpisy a vnitřními předpisy XXXXXX,
   2. evidence obsahuje alespoň tyto údaje:
      1. název programového vybavení,
      2. dodavatele nebo výrobce programového vybavení,
      3. počet pořízených licencí,
      4. druh licencí,
      5. platnost licencí,
      6. osobu odpovědnou za použití licencí,
   3. za distribuci, instalaci, údržbu, změny, rozvoj a vyřazování programového vybavení odpovídají Garanti podpůrných aktiv,
   4. nasazení programového vybavení je v souladu s licenčními podmínkami a zvláštním právním předpisem[[12]](#footnote-12)).
2. Pravidla a postupy pro kontrolu dodržování licenčních podmínek:
   1. proces kontroly dodržování licenčních podmínek je řízen a dokumentován,
   2. pravidelnou kontrolu dodržování licenčních podmínek včetně návrhu na nápravné opatření provádí Bezpečnostní správce.

### Způsoby ochrany elektronické výměny informací

1. Na ochranu elektronicky předávaných informací jsou použita opatření v souladu s politikou organizačních opatření – článek 8 „Politika řízení aktiv“, kde je uveden postup pro stanovení hodnoty aktiv z pohledu jejich důvěrnosti.
2. Informace publikované na veřejně přístupných IS (webové stránky XXXXXX) je nutno chránit proti neoprávněné modifikaci.

## Politika fyzické bezpečnosti

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je zajistit bezpečný provoz prostředků pro zpracování informací, služeb a procesů v souladu s bezpečnostními požadavky a potřebami.

### Pravidla pro ochranu objektů

1. Z hlediska fyzické ochrany je stanovena a dokumentována kategorizace prostor a minimální rozsah organizačních opatření a rozsah systémů technické ochrany, ve kterých jsou umístěny prvky ICT:
   1. prostory kategorie I – společné prostory, ve kterých jsou umístěny prvky ICT XXXXXX,
   2. prostory kategorie II – uzamykatelné kanceláře a místnosti, ve kterých jsou umístěny pracovní stanice,
   3. prostory kategorie III – režimové technologické místnosti, ve kterých jsou umístěny podružné rozvaděče se síťovými prvky vnitřní sítě,
   4. prostory kategorie IV – režimové serverovny a datová centra.
2. Kategorie konkrétních prostor určují Garanti příslušných aktiv.
3. Narušení fyzické bezpečnosti IS se považuje za BU případně za BI a je zaznamenáno do nástroje pro sběr a vyhodnocení bezpečnostních událostí.

### Pravidla pro kontrolu vstupu osob

Pravidla pro kontrolu vstupu do prostor s prvky ICT jsou stanovena v dokumentaci jednotlivých prostor dle kategorií v odstavce 21.2.

### Pravidla pro ochranu zařízení

Pravidla pro ochranu prvků ICT jsou stanovena v technické dokumentaci prvků ICT dle kategorií v článku 21.2.

### Detekce narušení fyzické bezpečnosti

1. Pravidla pro detekci narušení fyzické bezpečnosti jsou stanovena v bezpečnostní dokumentaci dle kategorií v článku 21.2.
2. Monitorování prostor s prvky ICT a detekce narušení prostor je v působnosti XXXXXX.

## Politika bezpečnosti komunikační sítě

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je stanovit způsob ochrany komunikačních sítí XXXXXX.

### Pravidla a postupy pro zajištění bezpečnosti sítě

1. Každá část komunikační sítě musí být dokumentovaná ve fyzické a logické vrstvě. Za vedení dokumentace odpovídá Bezpečnostní správce příslušného aktiva.
2. Správa sítě a síťových prvků je oddělena od správy pracovních stanic a serverů.
3. Síť je segmentována a logicky oddělena za účelem zajištění bezpečnosti prvků ICT systémů a odolnosti vůči případným útokům.

### Určení práv a povinností za bezpečný provoz sítě

1. Garant podpůrného aktiva je odpovědný za efektivní využití všech dostupných bezpečnostních funkcí používaných technologií.
2. Garant podpůrného aktiva stanoví odpovědnosti za správu bezpečnosti sítě.
3. Garant podpůrného aktiva zajistí dodržení principu oddělení rolí správy sítí a správy IS.

1. Architekt KB posuzuje nastavení a změny bezpečnosti provozu sítě a navrhuje opatření k zajištění bezpečného provozu sítě.

### Pravidla a postupy pro řízení přístupů v rámci sítě

1. Pravidla jsou aplikovatelná na všechny komunikační sítě ve správě XXXXXX alespoň v rozsahu:
   1. interní sítě LAN (včetně SAN),
   2. externí sítě WAN a MAN,
   3. propojení na externí sítě (Internet).
2. Pravidla pro řízení přístupu se aplikují na všechny segmenty sítě LAN.
3. Pro přístupy uživatelů a administrátorů do vnitřní sítě jsou použity nástroje pro správu a ověření identity.
4. Pro přístupy technických prostředků do vnitřní sítě jsou použity nástroje pro správu přístupu technických prostředků.
5. Přístupy jsou řízeny v jednotlivých prvcích ICT na základě skupin a rolí.

### Pravidla a postupy pro ochranu vzdáleného přístupu k síti

1. Vzdálený přístup uživatelů k sítím je řízen prostřednictvím odpovídajících technických prostředků.
2. Přístup z externích sítí je možný jen do demilitarizovaných zón (DMZ) navržených tak, aby případný vnější útok neohrozil bezpečnost interní sítě.
3. Vzdálený přístup je možný jen prostřednictvím komunikačního kanálu chráněného kryptografickými prostředky.
4. Vzdálené připojení dodavatelů je možné jen na základě oboustranné dohody, jejímž obsahem je povinně vzájemně akceptovaná bezpečnostní politika a výsledky analýzy rizik vyplývající z tohoto připojení.
5. Ověření identity žadatele o vzdálený přístup je provedeno formou vícefaktorové autentizace.

### Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů

1. Prvky ICT jsou trvale monitorovány.
2. Záznamy událostí prvků ICT je nutné uchovávat nejméně po dobu vyžadovanou zvláštním právním předpisem[[13]](#footnote-13)), nejméně však po dobu 12 měsíců.
3. Záznamy událostí musí být zajištěny před neoprávněným přístupem a neoprávněnou modifikací.
4. Všechny prvky ICT jsou napojeny na určený zdroj přesného času a jsou nejméně jednou za den synchronizovány.

## Politika ochrany před škodlivým kódem

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je stanovit postup pro minimalizaci rizik spojených s průnikem škodlivého kódu nebo jiného nežádoucího škodlivého programového prostředku.

### Pravidla a postupy pro ochranu síťové komunikace

1. Ochrana síťové komunikace je systémově zajištěna a průběžně aktualizována souborem technologických prostředků v celé síti XXXXXX.
2. Nastavení a procesy změn nástroje pro ochranu síťové komunikace jsou dokumentovány a řízeny.
3. Kontrola komunikace mezi jednotlivými segmenty sítě je realizována nástrojem pro ochranu před škodlivým kódem a jsou aplikována opatření pro prevenci a detekování škodlivých programových kódů.
4. Záznamy událostí z nástroje pro ochranu síťové komunikace jsou centrálně ukládány.
5. Garant podpůrných aktiv odpovídá za realizaci ochrany síťové komunikace před škodlivým kódem.

### Pravidla a postupy pro ochranu serverů a sdílených datových úložišť

1. Ochrana serverů a sdílených datových úložišť je zajištěna centrálním nástrojem pro ochranu před škodlivým kódem a jsou aplikována opatření pro prevenci a detekování škodlivých programových kódů.
2. Nastavení a procesy změn nástroje pro ochranu serverů a sdílených datových úložišť jsou dokumentovány a řízeny.
3. Jsou nastavena opatření pro detekci, prevenci a obnovu infikovaných dat, s upřednostněním smazání zavirovaného souboru před jeho léčbou.
4. Záznamy událostí (detekce škodlivého kódu) z nástrojů pro ochranu serverů a sdílených datových úložišť jsou centrálně ukládány.
5. Garant podpůrných aktiv odpovídá za realizaci ochrany serverů a sdílených datových úložišť před škodlivým kódem.

### Pravidla a postupy pro ochranu pracovních stanic

1. Nástroj pro ochranu před škodlivým kódem je součástí programového vybavení každé pracovní stanice a je pravidelně a centrálně aktualizován.
2. Jsou nastavena opatření pro detekci, prevenci a obnovu infikovaných dat s upřednostněním smazání zavirovaného souboru před jeho léčbou.
3. Záznamy událostí (detekce škodlivého kódu) z nástroje pro ochranu pracovních stanic jsou centrálně ukládány.
4. Uživatelům je zakázáno měnit na pracovní stanici konfiguraci nástroje pro ochranu před škodlivým kódem.
5. Zásady ochrany před škodlivým kódem jsou součástí zvyšování bezpečnostního povědomí uživatelů.
6. Garant podpůrných aktiv odpovídá za centrální distribuci a aktualizaci nástroje pro ochranu pracovních stanic před škodlivým kódem.

## Politika bezpečného používání kryptografické ochrany

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je stanovení pravidel bezpečného používání kryptografické ochrany.

### Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu

1. Úroveň ochrany s využitím kryptografického algoritmu je dokumentována a řízena pro každý prvek ICT.
2. Na základě analýzy rizik primárních aktiv je stanovena požadovaná úroveň ochrany s ohledem na:
   1. kategorizaci informací primárních aktiv,
   2. použití přenosového média,
   3. typ a sílu kryptografického algoritmu.

### Pravidla kryptografické ochrany informací

1. Pravidla pro použití kryptografické ochrany jsou dokumentována a řízena.
2. Aktualizace kryptografických algoritmů je prováděna minimálně v souladu s doporučením Úřadu.
3. Pro vybrané prvky ICT jsou používána kryptografická opatření za účelem zajištění:
   1. identifikačních a autentizačních prostředků,
   2. autorizačních prostředků,
   3. přenosu informací mezi prvky ICT,
   4. šifrování souborů,
   5. zabezpečení elektronické pošty a přístupu k internetu.
4. Opatření kryptografické ochrany informací jsou implementována po komunikačních sítích:
   1. mezi segmety sítí XXXXXX,
   2. při přístupu do vnitřní sítě XXXXXX z vnějšho prostředí,
   3. při výměně informací mezi IS.

1. Opatření kryptografické ochrany informací jsou implementována při uložení souborů na mobilní zařízení nebo vyměnitelné technické nosiče dat a je použita jedna z těchto metod:
   1. šifrování na úrovni celých disků,
   2. šifrování na úrovni virtuálních disků,
   3. šifrování na úrovni souborů.

### Systém správy klíčů

1. Systém správy klíčů je rozdělen na oblast:
   1. centrální správa klíčů,
   2. zaměstnanecké kryptografické klíče,
   3. kryptografické klíče systémových účtů,
   4. kryptografické klíče certifikačních autorit.

1. Systém centrální správy klíčů zajišťuje vydávání certifikátů a klíčů, jejich obnovu, zneplatnění a archivaci na úrovni XXXXXX.
2. Zaměstnanecké kryptografické klíče jsou používány výhradně pro:
   1. autentizaci ve vnitřní síti a vytváření interního elektronického podpisu,
   2. vytváření kvalifikovaného elektronického podpisu v souladu se zvláštními právními předpisy[[14]](#footnote-14)).
3. Kryptografické klíče systémových účtů slouží k šifrování dat na úrovni prvků ICT a k šifrování přenosu dat mezi prvky ICT.
4. Technické parametry importu kryptografických klíčů od kvalifikovaných poskytovatelů certifikačních služeb jsou stanoveny na základě smluvního vztahu mezi XXXXXX a kvalifikovaným poskytovatelem certifikačních služeb.

## Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událost

### Předmět úpravy

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je stanovit pravidla nasazení a používání nástroje pro detekci BU a systém bezpečnostních opatření.

### Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí

1. Pro detekci BU jsou stanovena pravidla pro zaznamenávání událostí, která jsou dokumentována a řízena.
2. Nástroj pro detekci BU zajišťuje sběr informací o provozních a bezpečnostních událostech a ochranu získaných informací před neoprávněným využitím nebo jejich změnou.
3. Nástroj pro detekci BU umožňuje poskytování informací pro určené bezpečnostní role o detekovaných bezpečnostních událostech.
4. Nástroj pro detekci BU umožňuje automatickou detekci známých zranitelností včetně pravidelné aktualizace.
5. Nástroj je nastaven ke sběru a zaznamenání bezpečnostních a provozních událostí alespoň v rozsahu:
   1. datum a čas vzniku události,
   2. typ činnosti provedené v prvku ICT,
   3. identifikace prvku ICT aktiva, které činnost zaznamenalo,
   4. identifikace účtu, pod kterým byla činnost provedena,
   5. síťová identifikace zařízení původce události,
   6. úspěšnost nebo neúspěšnost provedené činnosti v prvku ICT,
   7. přihlášení a odhlášení ke všem účtům včetně neúspěšných pokusů,
   8. činnosti provedené administrátory,
   9. manipulace s účty, včetně autentizace nebo autorizace,
   10. neprovedení činností v prvku ICT v důsledku nedostatku přístupových oprávnění,
   11. zahájení a ukončení činností technických aktiv,
   12. chybová hlášení technických aktiv,
   13. přístupy k záznamům o událostech, pokusy o manipulaci se záznamy o událostech  
       a změny nastavení nástroje pro zaznamenávání událostí.
6. Záznamy událostí prvků ICT se povinně uchovávají nejméně po dobu 12 měsíců souladu se zvláštním právním předpisem[[15]](#footnote-15)).
7. Všechny prvky ICT jsou napojeny na určený zdroj přesného času a jsou alespoň jednou za den synchronizovány.
8. Garant podpůrného aktiva je odpovědný za využití nástroje pro detekci BU ve XXXXXX.

### Postupy pro vyhodnocování a reakce na detekované kybernetické bezpečnostní události

1. Ve XXXXXX je používán nástroj pro sběr a vyhodnocování BU[[16]](#footnote-16)) s cílem identifikovat BI.
2. Nástroj pro správu a řešení provozních událostí, BU a BI je jednotným kontaktním místem.
3. Nástroje uvedené v odst. 1 a 2 poskytují informace pro určené provozní a bezpečnostní role o detekovaných BU, včetně včasného varování.
4. Proces řešení BU a BI je dokumentován a řízen.
5. Garant podpůrného aktiva je odpovědný za provoz nástroje pro detekci BU a nástroje pro správu a řešení provozních událostí, BU a BI.

### Pravidla pro optimalizaci nastavení nástroje pro detekci kybernetických událostí

1. Potenciální hrozby jsou v nástroji pro detekci BU zpracovávány a vyhodnocovány.
2. V případě zjištění neopodstatněné reakce nástroje pro detekci BU na událost, která není bezpečnostně relevantní, je nutno detekční pravidla nástroje pro detekci BU upravit.
3. V případě zjištění, že událost není indikována jako chyba, přestože se o chybu jedná a je nutno na ni reagovat, jsou upravena detekční pravidla nástroje pro detekci BU.
4. Za optimalizaci nastavení nástroje pro detekci BU je odpovědný Garant tohoto nástroje ve spolupráci s Architektem KB a Manažerem KB.

## Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

### Předmět

Účelem této části Politiky organizačních a technických opatření kybernetické bezpečnosti je stanovit pravidla využití a údržby nástroje pro sběr a vyhodnocení BU.

### Pravidla a postupy pro evidenci a vyhodnocení bezpečnostních událostí

1. Pro evidenci a vyhodnocení je využíván nástroj pro správu a řešení provozních událostí, BU a BI, který je současně jednotným kontaktním místem.
2. Nástroj pro správu a řešení provozních událostí, BU a BI poskytuje informace pro určené bezpečnostní role, uživatele a dodavatele. Přístup k těmto informacím je řízen na základě přístupových oprávnění.
3. V případě vyhodnocení neopodstatněné reakce nástroje na událost, která není bezpečnostně relevantní, jsou upravena detekční pravidla nástroje pro detekci BU.
4. V případě vyhodnocení, že událost není indikována jako chyba, ale de facto se o chybu jedná a musí být reagováno, jsou upravena detekční pravidla nástroje pro detekci BU.
5. Za evidenci a vyhodnocení BU a BI je odpovědný Manažer KB ve spolupráci s Architektem KB a Garanty aktiv.

### Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení bezpečnostních událostí

1. Pravidla a postupy určené k řešení BU a BI jsou řízeny, dokumentovány a pravidelně analyzovány, revidovány a aktualizovány, včetně definice, klasifikace a kategorizace.
2. Aktualizace pravidel a postupů vyhodnocování BU a BI je prováděna nástrojem pro sběr a vyhodnocení BU nebo na základě analýzy rizik jednotlivých aktiv.
3. Za aktualizaci nastavení bezpečnostních pravidel pro vyhodnocení BU a BI je odpovědný Bezpečnostní správce ve spolupráci s Architektem KB a Manažerem KB.

### Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení bezpečnostních událostí

1. Pravidla a postupy pro optimalizaci bezpečnostních vlastností nástroje pro sběr a vyhodnocení BU jsou dokumentovány a řízeny a jsou v souladu s aktuálním nastavením aktiv zaznamenaných v evidenci aktiv.
2. Optimalizace nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení BU je prováděna pro všechny prvky ICT s cílem předcházení BU.
3. Za optimalizaci nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení BU je odpovědný Manažer KB ve spolupráci s Architektem KB a Bezpečnostními správci.

…………………………………..

XXXXXX

…………………………………

XXXXXX

1. *) Příloha č. 5 Vyhlášky 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).* [↑](#footnote-ref-1)
2. *) § 6 a § 7 vyhlášky 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).* [↑](#footnote-ref-2)
3. ) *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).* [↑](#footnote-ref-3)
4. ) Národní úřad pro kybernetickou a informační bezpečnost [↑](#footnote-ref-4)
5. ) příloha č. 4 k vyhlášce o kybernetické bezpečnosti [↑](#footnote-ref-5)
6. ) *Příloha č. 6, tab. 5 vyhlášky 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).* [↑](#footnote-ref-6)
7. ) *Příloha č. 4 vyhlášky 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).* [↑](#footnote-ref-7)
8. *) Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.* [↑](#footnote-ref-8)
9. *) Zákon č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů.* [↑](#footnote-ref-9)
10. ) *Příloha č. 7 vyhlášky 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).* [↑](#footnote-ref-10)
11. ) *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).* [↑](#footnote-ref-11)
12. ) *Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů.* [↑](#footnote-ref-12)
13. ) *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).* [↑](#footnote-ref-13)
14. ) *Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.*

    *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 (eIDAS).*

    *Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů.* [↑](#footnote-ref-14)
15. *) § 22 vyhlášky 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).* [↑](#footnote-ref-15)
16. *) §§ 23-24 vyhlášky o kybernetické bezpečnosti.* [↑](#footnote-ref-16)