**(PK)**

projektu

Národní informační systém integrovaného záchranného systému (NIS IZS)

část

**F. Bezpečnostní projekt**

Dokument obsahuje: Vymezení rozsahu projektu z hlediska bezpečnosti, specifikaci rizik, zajištění fyzické a komunikační, kybernetické a personální bezpečnosti a její testování a přehled bezpečnostní dokumentace.

Verze: 5.1b

Schválil za Dodavatele: RNDr. Vladimír Příbramský

Datum aktualizace: 17/4/2014

Obsah

[01. Metodika 4](#_Toc385333728)

[Předpoklady 4](#_Toc385333729)

[Koncepce informační bezpečnosti NIS IZS 4](#_Toc385333730)

[02. Vymezení rozsahu NIS IZS 6](#_Toc385333731)

[Subjekty NIS IZS 6](#_Toc385333732)

[Data NIS IZS 6](#_Toc385333733)

[Provozní data NIS IZS 6](#_Toc385333734)

[Geografická data z veřejných zdrojů 6](#_Toc385333735)

[Geografická data z ostatních zdrojů 6](#_Toc385333736)

[Data od vybraných poskytovatelů 6](#_Toc385333737)

[Data pro správu NIS IZS 7](#_Toc385333738)

[Záznamy o provozu NIS IZS 7](#_Toc385333739)

[Software NIS IZS 7](#_Toc385333740)

[Hardware NIS IZS 7](#_Toc385333741)

[Lokality NIS IZS 7](#_Toc385333742)

[03. Řízení rizik NIS IZS 8](#_Toc385333743)

[Identifikace a klasifikace rizik 8](#_Toc385333744)

[Hodnocení rizik 9](#_Toc385333745)

[Zvládání rizik 9](#_Toc385333746)

[04. Fyzická bezpečnost 12](#_Toc385333747)

[Fyzická bezpečnost DC NIS 12](#_Toc385333748)

[Fyzická bezpečnost KDC NIS 14](#_Toc385333749)

[Fyzická bezpečnost zařízení NIS IZS 14](#_Toc385333750)

[05. Technická a komunikační bezpečnost 15](#_Toc385333751)

[Bezpečnost sítí v CDC a KDC NIS IZS 15](#_Toc385333752)

[Bezpečnost propojení mezi komponentami NIS IZS 15](#_Toc385333753)

[Bezpečnost připojení cizích zařízení k NIS IZS 19](#_Toc385333754)

[Bezpečnost připojení vlastních zařízení k NIS IZS 19](#_Toc385333755)

[Bezpečnost záložního propojení 20](#_Toc385333756)

[Připojení do Internetu 23](#_Toc385333757)

[Řízení privilegovaného přístupu k systému 24](#_Toc385333758)

[Řízení změn v systému 24](#_Toc385333759)

[Správa systému 25](#_Toc385333760)

[Řízení kontinuity a obnova po havárii 25](#_Toc385333761)

[06. Kybernetická bezpečnost NIS IZS 27](#_Toc385333762)

[Bezpečnostní monitoring NIS IZS 27](#_Toc385333763)

[Ochrana proti virům a škodlivému kódu 29](#_Toc385333764)

[Analýza technických zranitelností 29](#_Toc385333765)

[Zálohování a archivace 29](#_Toc385333766)

[07. Personální a organizační bezpečnost 31](#_Toc385333767)

[Personální bezpečnost 31](#_Toc385333768)

[Organizace bezpečnosti 32](#_Toc385333769)

[Řízení bezpečnostních incidentů 32](#_Toc385333770)

[08. Testování bezpečnosti NIS IZS 33](#_Toc385333771)

[Testování bezpečnosti aplikací 33](#_Toc385333772)

[Testování bezpečnosti infrastruktury 34](#_Toc385333773)

[Kontroly souladu 37](#_Toc385333774)

[09. Bezpečnostní dokumentace pro provoz 38](#_Toc385333775)

[Příloha 39](#_Toc385333776)

[Rejstřík 39](#_Toc385333777)

# Metodika

## Předpoklady

V textu je použito označení Dodavatel pro dodavatele projektu NIS IZS jak pro označení dodavatele v roli dodavatele NIS IZS, tak v roli budoucího provozovatele NIS IZS. Dodavatel popsanými činnostmi nepřijímá žádné závazky pro dobu, kdy nebude provozovatelem NIS IZS.

Řešení informační bezpečnosti NIS IZS popsané v tomto dokumentu vychází z následujících předpokladů:

* Předmětem ochrany nejsou data klasifikovaná podle zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
* Pro komunikaci je použita bezpečná síť ITS.
* Bezpečnostní opatření tvoří provázaný celek. Při změně nebo vynechání jednoho opatření musí být prozkoumán a vyhodnocen vliv změny na celkovou bezpečnost NIS IZS.

## Koncepce informační bezpečnosti NIS IZS

NIS IZS je navržen a budován jako vysoce bezpečný informační a komunikační systém. Důraz je kladen na všechny základní složky bezpečnosti informací.

* **Dostupnost**: informace jsou dostupné v požadovaném čase a na požadovaném místě. V případě NIS IZS se jedná o kritický požadavek.
* **Integrita**: pouze oprávněné subjekty mohou informace vytvářet a měnit.
* **Důvěrnost**: pouze oprávněné subjekty mohou informace číst.
* **Nepopiratelnost**: subjekt, který provedl nějakou operaci s informacemi, se nemůže vzdát odpovědnosti za provedení akce.

Dodavatel chápe informační bezpečnost NIS IZS jako proces. V etapě přípravy a realizace budou navržena a implementována určitá bezpečnostní opatření.

Během provozu bude Dodavatel identifikovat případné nové hrozby ohrožující systém a případné nové zranitelnosti systému a navrhne a realizuje **preventivní opatření** proti novým hrozbám a bude odstraňovat nové zranitelnosti**.**

Dodavatel budečinnost systému kontinuálně a v reálném čase monitorovat, mj. s cílem **detekovat** případná **narušení bezpečnosti**. Pokud se taková narušení vyskytnou, přijme **nápravná opatření a navrhne zvýšení bezpečnosti systému**. Monitoring bude provádět dohledové centrum Dodavatele.

Při řízení informační bezpečnosti NIS IZS bude Dodavatel dodržovat následující **principy**:

* Bezpečnost je založena na zvládání rizik, tj. na identifikaci rizik a realizaci odpovídajících opatření proti nim.
* Bezpečnost je a bude Dodavatelem řešena ve fázi přípravy NIS IZS pro provoz a v provozu v době, kdy Dodavatel bude provozovatelem NIS IZS.
* Jsou definovány a personálně obsazeny bezpečnostní role pro provoz a správu NIS IZS a vymezeny povinnosti osob, které budou jednotlivé role vykonávat.
* Je kontinuálně a v reálném čase monitorována bezpečnost provozu NIS IZS. Jsou definovány postupy pro vyšetřování bezpečnostních událostí a incidentů a zajištěny mechanismy pro přijetí nápravných opatření.
* Je zajištěna kontinuita činností NIS IZS při narušení systému, zejména pak výskytu následujících situací: při výpadcích jednotlivých zařízení potřebných pro provoz NIS IZS a při výpadcích jednotlivých centrálních DC a krajských DC NIS.
* Ze strany Zadavatele i Dodavatele jsou respektovány specifické bezpečnostní požadavky kladené na NIS IZS.
* Existuje a v průběhu provozu systému Dodavatel udržuje plán rozvoje NIS IZS pokrývající realizaci bezpečnostních opatření, která vyplývají z vyhodnocení incidentů, ze změn v charakteristice a hodnotách rizik a z návrhů na zvýšení bezpečnosti systému a jeho prostředí.

# Vymezení rozsahu NIS IZS

Do rozsahu NIS IZS patří:

* Subjekty NIS IZS
* Data NIS IZS
* Služby NIS IZS
* Software NIS IZS
* Hardware NIS IZS
* Lokality NIS IZS
* Síť NIS IZS

## Subjekty NIS IZS

Subjekty NIS IZS tvoří dvě skupiny – uživatelé a správci. Uživatelé jsou osoby používající NIS IZS. Jejich role jsou definovány v části „I - Školení“. Správci jsou osoby na straně Dodavatele NIS IZS, které provádějí administraci, monitoring, dohled a podporu 1. a 2. úrovně celého systému NIS IZS.

## Data NIS IZS

Data NIS IZS jsou rozdělena do následujících skupin:

### Provozní data NIS IZS

1. Záznamy o hovorech na tísňových linkách.
2. Údaje posílané z příjmu tísňového volání v KDC na krajská operační střediska.
3. Údaje posílané z krajských operačních středisek na příjem tísňového volání v KDC.

### Geografická data z veřejných zdrojů

1. Geodata ČÚZK.
2. Mapová díla ISKN.
3. RÚIAN.
4. Digitální mapa veřejné správy (až bude vytvořena a poskytnuta).

### Geografická data z ostatních zdrojů

1. ZABAGED.
2. Geonames.

### Data od vybraných poskytovatelů

1. Údaje poskytované telefonními operátory. Specifikovány v části J Prováděcího konceptu.
2. JSDI.
3. Údaje o meteorologické situaci. Poskytuje ČMHÚ, jde o neveřejné údaje.
4. Údaje o dopravní situaci. Poskytuje CDI prostřednictvím Policie ČR, jde o neveřejné údaje.

### Data pro správu NIS IZS

1. Konfigurační data síťových zařízení v DC.
2. Konfigurační data síťových zařízení na krajích. Včetně konfiguračních dat směrovačů CE pro připojení KDC a krajských operačních středisek k ITS.
3. Konfigurační data aplikace: definice procesů, definice pravidel.
4. Definice pravidel pro směrování zpráv.
5. Data posílaná dohledovými systémy.
6. Obsah komunikace správců s jednotlivými zařízeními.

### Záznamy o provozu NIS IZS

1. Logy.
2. Auditní záznamy.

## Software NIS IZS

Software je podrobně specifikováno v části B Prováděcího konceptu.

## Hardware NIS IZS

Hardware je podrobně specifikován v části A Prováděcího konceptu.

## Lokality NIS IZS

Lokality jsou podrobně specifikovány v příloze 1 části A Prováděcího konceptu.

# Řízení rizik NIS IZS

## Identifikace a klasifikace rizik

Následující rizika rozdělená do kategorií jsou uvažována jako základní seznam pro fázi provozu NIS IZS. Systém bude kontinuálně monitorovaný a budou sledována všechna potenciální rizika, která mohou být identifikována i mimo níže uvedený seznam.

**Fyzická rizika**

1. Ohrožení zařízení NIS IZS přírodními vlivy (záplavy, vítr, sníh, zemětřesení, blesk).
2. Ohrožení zařízení NIS IZS ohněm.
3. Ohrožení zařízení NIS IZS průmyslovými haváriemi.
4. Ohrožení zařízení NIS IZS nevyhovujícími podmínkami pro provoz (teplota, vlhkost, prašnost, stabilita dodávané elektřiny).
5. Krádež zařízení nebo jejich zničení či poškození.
6. Teroristický útok.

**Personální rizika**

1. Chyba obsluhy: chybné konfigurace hardware nebo software, chybné příkazy administrátorů. Chyby v DNS, směrování, IP adresách.
2. Sociální inženýrství proti osobám podílejícím se na provozu nebo správě NIS IZS s cílem zneužít jejich oprávnění.
3. Provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů nebo správců.

**Kybernetická rizika**

1. Výskyt škodlivého software, např. viry, spyware, trojské koně apod v NIS IZS.
2. Kybernetický útok vedený proti NIS IZS z nějaké vnější sítě (ITS, CMS, KSP) - footprinting, lámání hesel, spouštění kódu.
3. Útok na dostupnost NIS IZS z nějaké vnější sítě (ITS, CMS, KSP).
4. Kybernetický útok vedený proti NIS IZS z vnitřní sítě (NIS) - footprinting, lámání hesel, spouštění kódu.
5. Útok na dostupnost NIS IZS z vnitřní sítě (NIS).
6. Falšování identity uživatele nebo zařízení.

**Technická rizika**

1. Chyba aplikačního software.
2. Nedostupnost dat potřebných pro fungování aplikací.
3. Použití neověřených dat potřebných pro fungování aplikací.
4. Neoprávněná modifikace nebo smazání dat NIS.
5. Infiltrace komunikace, narušení integrity přenášených dat NIS.
6. Zneužití dat NIS, neoprávněný přístup k datům NIS, neoprávněné kopírování dat NIS.
7. Zachycení komunikace, narušení důvěrnosti přenášených dat NIS.
8. Chyba systémového software.
9. Selhání nebo neúmyslné poškození hardware.
10. Nedostupnost komunikací (počítačové sítě, telefonní síť).
11. Přerušení dodávky elektrické energie.
12. Využívání software v rozporu s licenčními podmínkami.

## Hodnocení rizik

Dodavatel provedl hodnocení rizik, ve kterém vyhodnotil jednotlivá rizika a navrhl opatření na jejich pokrytí, odstranění nebo snížení jejich míry. Opatření tvoří základ tohoto dokumentu a jsou popsána v jeho jednotlivých kapitolách jako požadavky na zajištění bezpečnosti. Hodnocení informačních rizik a návrh protiopatření je klíčovou částí řízení bezpečnosti informačních systémů obecně a tedy i NIS IZS.

Cílem hodnocení rizik je stanovení závažnosti jednotlivých rizik a zajištění, že aktuálně navržená bezpečnostní opatření jsou dostatečná a efektivní.

Rizika budou vyhodnocována kontinuálně v rámci celého životního cyklu NIS IZS. Během hodnocení rizik může být zjištěno, že některá rizika vykazují při aktuálně navržených opatřeních příliš vysokou míru. Pokud taková situace nastane, Dodavatel navrhne způsob zvládnutí rizika.

## Zvládání rizik

Existuje několik metod pro zvládnutí rizika existujícího i po realizaci navržených opatřeni. Tato rizika se nazývají zbytková rizika.

1. Pokrytí rizika, tady snížení jeho míry výběrem takových opatření (dosud nerealizovaných a nenavržených), aby mohlo být zbytkové riziko vyhodnoceno jako akceptovatelné trvale nebo dočasně.
2. Vědomé přijetí (akceptace) rizika se může použít v případě, že se nejedná o vysoké riziko a není vážně ohrožena bezpečnost informačních aktiv a jsou splněny požadavky zadavatele na bezpečnost informací.
3. Přenos rizika lze použít v případě, že je obtížné snížit riziko na přijatelnou úroveň vlastními zdroji. Možnými metodami je pojištění nebo outsourcing.
4. Vyhnutí se riziku znamená jakoukoli akci, při které jsou podmínky provozu informačního nebo komunikačního systému změněny tak, aby výskyt rizika nenastal.

Většina rizik bude pokryta opatřeními, která zajistí požadovanou úroveň bezpečnosti NIS IZS. Akceptace rizik, případně jeho přenos budou využity pouze za předpokladu, že nebudou znamenat porušení požadavků Zadavatele na bezpečnost NIS IZS a zákonných požadavků na bezpečnost NIS IZS.

Pro pokrytí rizik budou realizována bezpečnostní opatření, která jsou ekonomicky přiměřená a technicky dostupná a která budou mít následující formy:

1. Technická opatření.
2. Personální opatření.
3. Organizační opatření.
4. Bezpečnostní standardy v bezpečnostní politice NIS IZS.
5. Pracovní postupy používané při správě a užívání NIS IZS.

Cílem opatření je zajistit přiměřenou bezpečnost NIS IZS v následujících oblastech:

* Fyzická bezpečnost. Tato opatření zajišťují bezpečné umístění technických prostředků NIS IZS a omezení fyzického přístupu k zařízením NIS IZS. Mezi opatření fyzické bezpečnosti patří i zajištění bezpečných podmínek pro provoz technických zařízení NIS IZS včetně klimatizace, dostatečných prostor, pravidel pro údržbu a kontrolu přístupu k zařízení systému.
* Technická a komunikační bezpečnost. Tato opatření zahrnují implementaci bezpečnostních technologií, které zajistí kontinuální prosazení požadované úrovně bezpečnosti v celém systému po technické stránce. Technická bezpečnostní opatření vycházejí z bezpečnostních standardů a vynucují jejich dodržování uživateli a správci NIS IZS.
* Kybernetická bezpečnost. Tato opatření zajišťují bezpečnost dat v digitální formě při jejich zpracování, ukládání a přenosech včetně ochrany proti malware, hackerským útokům a jinému zneužití.
* Personální bezpečnost. Tato opatření zajišťují bezpečnost činnosti osob při provozu NIS IZS. Zahrnuje definice postupů pro různé činnosti, obsazování bezpečnostních rolí důvěryhodnými osobami (viz kapitolu „Personální bezpečnost“), povinnosti zachovávat mlčenlivost a bezpečnostní vzdělávání.
* Organizační bezpečnost. Tato opatření zajišťují jasnou definici kompetencí, práv a odpovědností jednotlivých rolí v systému na straně Zadavatele i Dodavatele.

Součástí návrhu řešení NIS IZS je řada bezpečnostních opatření. Během výběru opatření je důležité zvážit náklady na zavedení a provozování opatření ve vztahu k hodnotě chráněných aktiv. Dodavatel navrhne a implementuje taková protiopatření, která splní požadavky na zvládnutí rizik a budou respektovat existující finanční, časová a technická omezení.

V rámci dalších prací budou bezpečnostní požadavky uvedené v dalších kapitolách tohoto dokumentu transformovány do Registru bezpečnostních požadavků a opatření, který bude základním etalonem pro nastavení požadované úrovně bezpečnosti NIS IZS. Registr bude umožnovat sledování naplnění jednotlivých požadavků v průběhu vývoje, implementace i provozu NIS IZS. Registr bezpečnostních požadavků a opatření vytvoří a bude udržovat Dodavatel.

Detailní a kompletní návrh bezpečnostních opatření v registru, včetně plánu jejich implementace bude vytvořen v dalších fázích projektu. Opatření budou vycházet z ISO/IEC 27002, NIST 800-53 a dalších nejlepších praktik. V dalších kapitolách jsou uvedena základní opatření, která musí být realizována, nicméně jejich přesná technická specifikace je závislá mj. na konkrétních technologiích, které při tvorbě tohoto konceptu nejsou známé zcela nebo z části. Dodavatel bezpečnostní opatření detailně specifikuje v rámci dalších fází projektu (viz kap. 9. této části PKv40).

# Fyzická bezpečnost

Pojem „fyzická bezpečnost“ je používán ve smyslu zajištění bezpečných podmínek pro provoz technických zařízení. Zahrnuje jak opatření pro omezení fyzického přístupu k zařízením, tak pro zajištění provozních podmínek (teplota, vlhkost atd.) pro zařízení. Toto je ve shodě s terminologií používanou v návrhu zákona o kybernetické bezpečnosti a s terminologií používanou NBÚ (např. v zákoně č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů).

Opatření na omezení fyzického přístupu k zařízením tvoří základ bezpečnostních opatření. Pokud totiž útočník získá fyzický přístup k některým zařízením, stanou se bezpečnostní opatření proti určitým typům útoků neúčinná.

Běžná zařízení výpočetní techniky potřebují ke své činnosti přiměřené provozní podmínky, zejména určitou teplotu a vlhkost a omezenou prašnost. Pro spolehlivé fungování zařízení je důležité takové prostředí zajistit. Dále tato zařízení potřebují zásobování elektřinou a to v požadované úrovni a kvalitě. Kolísání proudu a napětí ovlivňuje negativně nejen životnost zařízení výpočetní techniky ale i jejich funkce. Správné funkce a prodloužení životnosti zařízení lze také zajistit pravidelnou údržbou podle pokynů výrobce. Proto Dodavatel věnuje v rámci fyzické bezpečnosti pozornost i zajištění potřebných provozních podmínek pro zařízení výpočetní techniky a jejich údržbě.

## Fyzická bezpečnost DC NIS

1. DC budou v budovách se řízeným přístupem a evidencí vstupujících osob. Kontrolu a evidenci budou provádět buď pracovníci recepce/vrátnice nebo bude prováděna automaticky pomocí technických zařízení.
2. Pro řízení přístupu do DC a prostor se zařízením NIS IZS jsou vytvořeny postupy a je udržován aktuální seznam pracovníků s oprávněným přístupem k zařízení NIS IZS.
3. Přístup do lokality a budovy DC bude monitorován.
4. V DC bude zajištěna požární ochrana.
5. DC budou chráněna proti živelným katastrofám.
6. DC nebudou umístěna v blízkosti nebezpečných průmyslových provozů (typu výroby výbušnin a velkých chemických podniků).
7. V budovách s DC nebudou provozy nebo zařízení způsobující vibrace instalovaných zařízení.
8. DC budou umístěna tak, aby nebyla ve zvýšené míře ohrožena pořádáním hromadných akcí (zejména demonstrací a sportovních akcí spojených s vandalismem) v jejich blízkosti.
9. Prostory se zařízeními NIS IZS budou monitorovány a záznamy budou uloženy a archivovány v souladu s požadavky Zadavatele a Dodavatele.
10. Prostory se zařízeními NIS IZS nebudou dostupné z veřejně přístupných prostor.
11. Systémy pro podporu zabezpečovacích a přístupových systémů budou umístěny mimo prostory, kde se nachází zařízení NIZ IZS. Přístup k zabezpečovacím a přístupovým systémům bude přísně řízen.
12. Prostory se zařízeními NIS IZS budou vybaveny proti elektromagnetismu a statické elektřině (antistatická podlaha).
13. Zařízení NIS IZS budou v rámci DC umístěna v prostorách oddělených od okolí. Stačí uzamykatelné skříně (rack).
14. Bude zajištěna fyzická ostraha DC. Ostraha DC bude mít povolen přístup do prostor se zařízeními NIS IZS pouze v případě mimořádných událostí a každý vstup ostrahy bude zaprotokolován. Mimořádnými událostmi se zde myslí následující události: požár, zaplavení, vysoká teplota, neoprávněný vstup.
15. Fyzický přístup k zařízením NIS IZS bude monitorován (např. prostřednictvím automatických záznamů otevření racků/skříní nebo organizačním opatřením – klíče k racku budou vydávány pouze oprávněným pracovníkům Dodavatele proti podpisu, případně budou práce na zařízení NIS IZS prováděny pod dohledem ostrahy DC).
16. Dodavatelem budou vytvořeny postupy pro nouzové opravy zařízení a jejich výměnu, či opravu na místě.
17. Prostory v DC pro zařízení NIS IZS budou splňovat požadavky zařízení na provozní podmínky (teplota, vlhkost) instalovaných zařízení podle údajů výrobce. Bude zajištěno instalací klimatizačních jednotek včetně zvlhčovačů vzduchu.
18. Bude zajištěn bezpečný přístup k jednotlivým zařízením a budou zajištěny dostatečné servisní prostory kolem nich (min. 0.5m mezi racky).
19. DC budou vybavena elektrickými silovými rozvody dostatečné kapacity a kvality dle specifikace, která bude upřesněna po výběru konkrétních technologií. Budou splněny minimálně následující požadavky:
    1. Elektrické kabely budou buď uloženy ve dvojité podlaze, nebo budou zakryté lištami.
    2. Bude zajištěna kvalita proudu a ochrana před kolísáním napětí. Napájení bude procházet přes záložní zdroj elektřiny, který potřebnou ochranu zajistí.
20. Bude zajištěno bezpečné zásobování všech zařízení NIS IZS v DC elektřinou. DC bude vybaveno UPS a centrálními záložními zdroji podle standardů A studie interoperability.
21. Bude omezen fyzický přístup k datovým rozvodům. Buď budou uloženy do lišt, nebo vedeny pod podlahou nebo pod stropem.

## Fyzická bezpečnost KDC NIS

Požadavky na bezpečnost jsou uvedeny ve standardech A Analýzy interoperability základních složek integrovaného záchranného systému.

## Fyzická bezpečnost zařízení NIS IZS

Vztahuje se na všechna zařízení NIS IZS nezávisle na jejich umístění.

1. Všechna zařízení NIS IZS budou provozována a udržována v souladu s doporučením výrobce. Veškeré opravy a servisní zásahy budou provádět pouze oprávněné osoby s potřebnou kvalifikací. Veškeré opravy a servisní zásahy budou prováděny pouze se souhlasem Dodavatele a za dozoru jeho zástupce nebo osoby pověřené Dodavatelem.
2. Budou vytvořeny postupy pro nouzové opravy zařízení a jejich výměnu, či opravu na místě. Opravy budou realizovány důvěryhodnými pracovníky s oprávněným přístupem.
3. Bude zajištěno bezpečné vymazání/přepsání obsahu paměťových médií používaných pro NIS IZS v případě jejich likvidace nebo zaslání do opravy.
4. Transport zařízení NIS IZS do opravy mimo lokalitu DC bude prováděn bezpečným způsobem, který zajistí Dodavatel. Dodavatelem budou vytvořeny postupy pro transport.
5. Je stále udržován aktuální seznam technického vybavení a jsou prováděny pravidelné kontroly souladu.

# Technická a komunikační bezpečnost

Opatření zahrnují implementaci bezpečnostních technologií a jejich nastavení, které zajistí kontinuální prosazení požadované úrovně bezpečnosti v celém systému po technické stránce. Technická bezpečnostní opatření vycházejí z bezpečnostních standardů a vynucují jejich dodržování uživateli a správci NIS IZS.

## Bezpečnost sítí v CDC a KDC NIS IZS

Pro zajištění bezpečnosti počítačových sítí v jednotlivých CDC a KDC NIS realizuje Dodavatel minimálně následující opatření:

1. Síťová zařízení NIS IZS budou umístěna pouze v chráněných a monitorovaných prostorech s řízeným přístupem.
2. Pro provoz a správu NIS IZS nejsou využívané bezdrátové sítě Wi-Fi.
3. Bude kontrolováno připojení zařízení k aktivním síťovým prvkům NIS IZS. Nepoužívané porty budou deaktivovány.
4. Bude prováděna autentizace zařízení připojených k aktivním síťovým prvkům NIS IZS, aby bylo zabráněno připojení neautorizovaných zařízení.
5. Zařízení v DC NIS IZS budou oddělena buď fyzicky nebo na L2 od zařízení, která nejsou určena pro provoz NIS IZS.

Fyzické oddělení znamená, že zařízení NIS IZS nejsou fyzicky připojena k jiným síťovým zařízením.

Oddělení na L2 znamená, že zařízení NIS IZS jsou provozována v různých VLAN. Za tohoto předpokladu je možné sdílet síťovou infrastrukturu s jinými systémy.

1. Zařízení v DC NIS IZS budou oddělena na L3 od všech ostatních zařízení umístěných v LAN.

Oddělení na L3 znamená, že zařízení různých subsystémů ZR jsou v různých IP sítích (IP subnets) a provoz mezi nimi musí být směrován (routing).

1. Logický přístup na administrační rozhraní síťových prvků je řízen a je omezen pouze na oprávněné a jednoznačně identifikovatelné správce systému.
2. U síťových zařízení jsou pro privilegované a neprivilegované činnosti používány samostatné účty.
3. Vzdálený přístup k síťovým zařízením je omezen pouze na jednoznačně identifikovatelné správce systému.
4. Konfigurační nastavení síťových zařízení jsou pravidelně zálohována.

## Bezpečnost propojení mezi komponentami NIS IZS

V této kapitole je řešena bezpečnost následujících propojení:

* komunikace operačních středisek NIS s CDC a KDC NIS,
* komunikace středisek operačního řízení IZS s CDC a KDC NIS,
* komunikace mezi CDC a KDC NIS.

**Firewally v CDC a KDC NIS**

Na operačních střediscích budou umístěna koncová zařízení pro práci s NIS IZS: telefony a pracovní stanice. Tato zařízení budou plně pod kontrolou Dodavatele a nebudou připojena do žádných dalších sítí.

V CDC a KDC budou umístěny servery a další zařízení potřebná pro provoz NIS (disková pole, zálohovací a archivační zařízení, atd.). Tato zařízení budou plně pod kontrolou Dodavatele a nebudou připojena do žádných dalších sítí s výjimkou telefonní ústředny, která bude připojena do VTS, ale od ní bude oddělena SIP firewallem.

Na střediscích operačního řízení budou umístěna zařízení jednotlivých složek IZS. Tato zařízení nebudou pod kontrolou Dodavatele.

K propojení bude použita zabezpečená síť ITS (viz část C „Síťová infrastruktura“).

S výjimkou středisek operačního řízení IZS budou ostatní komponenty pod kontrolou Dodavatele. Proto postačí bezpečnostně oddělit střediska operačního řízení IZS od CDC a KDC NIS. Toto oddělení bude provedeno **ve všech CDC a KDC NIS instalací firewallů**. Tyto firewally budou sloužit k filtraci datového i hlasového provozu mezi CDC a KDC NIS a okolím.

**Opatření v operačních střediscích NIS**

Na jednotlivých operačních střediscích NIS firewally nebudou, ale i tam budou nastavena následující bezpečnostní opatření na CE směrovačích.

1. Omezit komunikaci na předem definované a dokumentované IP adresy a protokoly.
2. Zajistit, aby komunikace z operačních středisek byla směrována pouze směrem do CDC NIS nebo KDC NIS.
3. Rozdělit VPN projektu NIS IZS do dvou částí: NIS „backplain“ a NIS „public“.
4. Umístit CDC a KDC projektu v části NIS „backplain“ (tato VPN zajišťuje komunikaci mezi jednotlivými systémy, klienti nemají mít do VPN NIS “backplain“ přístup)
5. Zajistit komunikaci v rámci VPN NIS „backplain“ řízeným prostupem výlučně pro požadované služby.
6. Nepovolit vypisování směrovacích údajů pro připojení do VPN NIS „backplain“.
7. Zajistit vzájemné oddělení a prostupy LAN připojených sítí KSP jednotlivých složek a krajů, což umožní odebírání potřebných služeb bez nutnosti budovat oddělenou LAN pro projekt NIS IZS.
8. Oddělit VPN NIS „backplain“ a VPN NIS „public“ (stejně tak jako pro hlasové VPN „Voice backplain“ a „Voice public“) a prostupy mezi nimi řídit pomocí ACL nebo firewallu.
9. Zakázat propagaci směrovacích informací ostatních subjektů IZS z VPN NIS „public“ do jednotlivých LAN složek IZS.
10. Ve VPN síti NIS „Voice pulic“ budou zapojeny telefonní aparáty projektu NIS IZS, výjimkou je HZS kde je tato VPN společná pro projekty NIS a KSP.
11. Použít pro řízení prostupů v rámci hlasových VPN sítí „Voice public“ a „Voice backplain“ prvky SBC (Session Border Controller). Viz část C - SÍŤ PKv51.
12. Omezit posílání ICMP na nezbytné případy.
13. Blokovat pakety s nastavenými IP options.
14. Blokovat pakety pokoušející se falšovat totožnost odesilatele (anti-spoofing).
15. Při výměně směrovacích informací používat autentizaci. Přijímat směrovací informace pouze ze známých bezpečných a jednoznačně identifikovatelných zdrojů. Zakázat source routing.
16. Omezit / zakázat broadcast a multicast, speciálně broadcast do nelokálních sítí.
17. Zakázat proxy ARP.
18. V odůvodněných případech použít pevné ARP záznamy.
19. Minimalizovat používání DNS.
20. Vypracovat postup pro rychlé a jednoduché zablokování jednotlivých VPN na síťových zařízeních.
21. Provádět pravidelné aplikace bezpečnostních aktualizací software síťová zařízení.
22. Požadovat jednoznačnou autentizaci pro přístup pracovníků k síťovým zařízením. Standardně používat AAA servery, ale pro nouzové případy povolit minimální počet privilegovaných účtů s lokální autentizací.
23. Nastavit autorizaci příkazů  zadávaných na příkazové řádce tak, aby bylo možné na AAA serveru sledovat příkazy zadávané administrátorem na síťovém zařízení.
24. Nepovolit logický přístup jakýchkoli osob mimo správců síťových zařízení a to ani pro read only přístup.
25. Používat zamykání účtů po neúspěšných pokusech o přístup k síťovým zařízením.
26. Používat ochranu proti resetování hesel.
27. Změnit všechna předdefinovaná hesla. Zrušit předdefinované účty, pokud je to možné.
28. Nastavit automatické odhlášení uživatele po určité době nečinnosti (max 5 min).
29. Pro přístup ke směrovači používat šifrované protokoly.
30. Všechny nepoužívané protokoly na síťovém zařízení vypnout.
31. Pro povolené protokoly omezit přístup k síťovým zařízením pomocí ACL pouze z vymezených rozsahů adres.
32. Pro SNMP nepoužívat implicitní community strings.
33. Použít SNMPv3.
34. Pro různé SNMP community omezit přístup k pouze nezbytným částem MIB.
35. Definovat bezpečné NTP servery pro synchronizaci času síťových zařízení.
36. Rezervovat část systémových prostředků (paměti a procesoru) pro administrátorský přístup.
37. Zapnout ochrany proti modifikaci software a konfigurací uložených v síťových zařízeních, pokud je na použitých zařízeních taková ochrana dostupná. Jedná se o digitální podpisy software, kontrolní součty a podobná opatření.
38. Zapnout ochrany proti útokům na úrovni dat, pokud je na použitých typech zařízení taková ochrana dostupná. Např. ochrana proti útokům typu buffer overflow.
39. K síťovým zařízením připojit IDS sondy založené na freeware (Snort). Sondy budou připojeny tak, že budou dostávat kopii veškerého provozu procházejícího síťovým zařízením a budou v něm sledovat známé útoky.

* Toto zapojení IDS sond je z hlediska zařízení v NIS IZS a zařízení ve VPN složek transparentní. Sonda může být kdykoli odebrána nebo připojena bez změny konfigurace ostatních zařízení.
* IDS sondy budou provozovány jako virtuální servery pod operačním systémem Linux. Nejsou tedy potřeba žádné licence.
* IDS sondy budou umístěny v KDC.
* Pokud IDS sonda nebude stíhat provádět inspekci veškerého provozu, neprojde příslušná část provozu inspekcí, ale síťový provoz tím nebude nijak narušen.
* IDS bude napojen na centrální (bezpečnostní) dohledový systém, který bude výskyt malware a anomálií v síťovém provozu hlásit.
* Výsledky monitoringu budou pravidelně vyhodnocovány a bezpečnostní manažer NIS IZS rozhodne podle výsledků po dohodě se Zadavatelem o realizaci dalších bezpečnostních opatření. Bezpečnostní manažer NIS IZS je osoba na straně Dodavatele pověřená dohledem nad bezpečností NIS IZS.

## Bezpečnost připojení cizích zařízení k NIS IZS

Systém NIS IZS bude provozován na zařízeních Dodavatele, zařízeních Dodavatelem spravovaných a hybridních pracovních stanicích. Připojení jiných zařízení není povoleno, pouze s výjimkou pro přístup k záznamům o provozu síťových zařízení za následujících podmínek:

* Na žádost příslušné složky IZS v určité lokalitě bude definován port na přepínači, ke kterému bude možné připojit zařízení spravované příslušnou složkou.
* Na tento port bude směrovač, respektive firewall posílat část informací o síťovém provozu.
* Pro předávání informací budou použity standardní protokoly syslog a SNMP traps. Zprávy syslog budou omezeny podle typu (facility) a závažnosti (severity). Posílat se budou pouze takové zprávy, které mají význam z hlediska řešení problémů na úrovni kraje. Obdobně budou omezeny SNMP traps.
* V bezpečnostní politice NIS IZS bude definován postup a podmínky, kdy má Dodavatel právo v případě problémů či bezpečnostních incidentů odpojit zařízení, která nejsou pod jeho správou, vyjma hybridních pracovních stanic.

## Bezpečnost připojení vlastních zařízení k NIS IZS

Na operačních střediscích budou k NIS IZS připojeny pouze pracovní stanice a telefony NIS, a případně zařízení, na které bude posílána informace o síťovém provozu.

V DC a KDC NIS budou k NIS IZS připojena pouze schválená zařízení, která budou pod kontrolou Dodavatele NIS. Systém bude schopen ověřit pomocí systému NAC, zda má připojené síťové zařízení právo připojit se k síti NIS IZS.

Pracovní stanice na operačních střediscích, vyjma hybridních pracovních stanic, budou pod kontrolou Dodavatele NIS a bude v nich pouze software nahrávaný z centrálního zdroje.

Telefony na operačních střediscích NIS budou pod kontrolou Dodavatele NIS (Dodavatel předpokládá součinnost ze strany složky PČR formou zajištění přístupu na CE směrovače).

Připojení neschváleného zařízení k NIS IZS bude kvalifikováno jako závažný bezpečnostní incident a proto budou realizována bezpečnosti opatření proti připojování neschválených zařízení k NIS IZS. Může se jednat buď o pokus připojit neschválené zařízení k nějakému nevyužitému portu aktivního síťového prvku, nebo o pokus o nahrazení schváleného zařízení neschváleným zařízením, nebo o pokus vydávat neschválené zařízení za schválené. Dodavatel zajistí kombinací následujících opatření.

* Kompletní kontrola nad telefonem. Technickými prostředky bude zabráněno modifikaci software a nahrávání vlastního software. Malware by musel být nahrán již při zavádění software do pracovní stanice / telefonu z centrálního zdroje.
* Pracoviště OŘ bude vybaveno takovými periferními zařízeními (myši, klávesnice, atd), které neposkytují aktivní rozhraní pro připojení datových médií (např. USB disky).
* VDI servery pro pracovní stanice OŘ (ZZS, PČR) budou umístěny PČR a ZZS v rámci VPN sítě NIS „public“, do této VPN sítě budou připojeny přes CE směrovače LAN složek IZS, kde jsou připojeny terminály/CPE.
* Autentizace zařízení připojených k jednotlivým portům aktivních síťových prvků. Dodavatel bude kombinovat následující metody autentizace.
  + Nechat aktivní prvek naučit se první MAC adresu pro každou VLAN („data“ / „voice“) a nepovolit na portu jiné MAC adresy.
  + Implementovat autentizaci pracovní stanice přímo do aplikace. V době, kdy aplikace na pracovní stanici není vytížená, bude centrální NIS IPL posílat aplikační „ping“. Aplikace na pracovní stanici musí reagovat očekávaným způsobem. Pokud nereaguje, znamená to, že buď je pracovní stanice nedostupná, nebo je připojeno jiné zařízení. Informace o tom, že příslušný port na aktivním prvku je aktivní a současně zařízení připojené k portu nereaguje správně na aplikační „ping“, se složí v bezpečnostním monitoringu (korelace dvou událostí).
  + Implementovat autentizaci telefonu přímo do aplikace. V době, kdy telefon není vytížený, bude centrální NIS IPL posílat aplikační „ping“. Telefon musí reagovat očekávaným způsobem. Pokud nereaguje, znamená to, že buď je telefon nedostupný, nebo je připojeno jiné zařízení. Informace o tom, že příslušný port na aktivním prvku je aktivní a současně zařízení připojené k portu nereaguje správně na aplikační „ping“, se složí v bezpečnostním monitoringu (korelace dvou událostí).
* Deaktivace všech nepoužívaných portů aktivních síťových zařízení.

## Bezpečnost záložního propojení

Pro případ výpadku ITS doporučuje Dodavatel, aby existovala možnost komunikace mezi operačními středisky a DC NIS přes CMS2. **Zřízení těchto linek není součástí projektu NIS IZS**. V této kapitole jsou uvedeny bezpečnostní požadavky na toto propojení.

Záložní propojení bude realizováno využitím standardních přípojek KIVS. Existuje několik různých situací lišících se místem a rozsahem výpadku ITS:

* + výpadek propojení z kraje k centrálním DC NIS,
  + výpadek ITS v rámci kraje,
  + výpadek napojení centrálních DC NIS,
  + výpadek celé ITS.

Základní schéma je uvedeno na následujícím obrázku. Kraj A je příklad kraje s fungující ITS v rámci kraje a bez připojení do centra. Kraj B je příklad kraje, kde funguje jak ITS v rámci kraje, tak propojení do centra. Kraj C je příklad kraje bez ITS na kraji.

Další komentáře k obrázku jsou dále v textu.

****

**Výpadek propojení z kraje k centrálním DC NIS**

V případě výpadku propojení ITS z kraje k centrálním DC NIS bude komunikace operačních středisek IZS s centrálními NIS přerušena a operační střediska budou spolu v rámci kraje komunikovat přes příslušné KDC NIS. Spojení mimo kraj není. V obrázku výše je to situace **kraje A**.

* Kraj A potřebuje ke své činnosti KDC kraje A.
* Mezi složkami IZS lze v rámci kraje komunikovat přes krajskou IPL umístěnou v KDC NIS kraje A.
* Se složkami IZS mimo kraj A nelze komunikovat.

**Výpadek ITS v rámci kraje**

V případě výpadku ITS v rámci kraje naváží operační střediska z příslušného kraje náhradní spojení s centrálními DC NIS přes linky KIVS a CMS2. Linky KIVS z jednotlivých složek IZS z jednotlivých krajů jsou do CMS2 přivedeny jako VPN příslušného operátora KIVS. V CMS2 jsou z těchto VPN operátorů KIVS vytvořeny službami CMS2 příslušné standardní VPN ITS „HZS\_data“, „PCR\_data“ a „ZZS\_data“. Provoz je těmito VPN předán do fungující centrální části ITS, která předá provoz centrální IPL ve VPN „NSPTV\_data“.

V obrázku výše je to situace **kraje C**.

* Kraj C nepotřebuje ke své činnosti KDC kraje D (to je nedostupné).
* Mezi složkami IZS lze v rámci kraje komunikovat přes centrální IPL umístěnou v DC NIS.
* Se složkami IZS mimo kraj C lze komunikovat přes CMS2. Tj. operační středisko HZS kraje C komunikuje s operačním střediskem kraje B přes CMS2 bez toho, aby provoz procházel přes centrální IPL. Toho je dosaženo standardní službou CMS2 „Vytvoření jedné VPN CMS2 z více VPN operátorů KIVS a ITS“. Tj. CMS2 spojí všechny VPN „HZS“ všech operátorů do jedné VPN „HZS\_data“ CMS2 a ITS.

**Výpadek napojení centrálních DC NIS**

V případě výpadku napojení jednotlivých centrálních DC NIS na ITS budou operační střediska IZS komunikovat se zbývajícími DC NIS, která zůstanou přes ITS připojena. V případě výpadku napojení všech DC NIS budou operační střediska komunikovat s KDC NIS ve svém kraji.

**Výpadek celé ITS**

Výpadek celé ITS je kombinací výše uvedených typů výpadků. Veškerá komunikace bude probíhat přes KIVS a CMS2.

**Pravidla**

* Každé operační středisko NIS IZS by mělo mít dle doporučení Dodavatele záložní spojení na DC NIS přes CMS2.
* Operační střediska jednotlivých složek IZS v případě výpadku spojení přes ITS na DC NIS přecházejí na vzájemnou komunikaci v rámci kraje přes IPL v KDC. Žádné záložní spojení z operačních středisek nebude aktivováno.
* Operační střediska se přepínají na záložní připojení k DC NIS v případě výpadku spojení přes ITS na DC NIS i na KDC NIS.
* Každé DC NIS má záložní připojení do CMS2.
* DC NIS se přepíná na záložní připojení v případě výpadku svého připojení k ITS.
* Dokud funguje připojení aspoň jednoho DC NIS k ITS, komunikují všechna operační střediska s těmi DC NIS, kterým připojení k ITS funguje.
* KDC NIS žádná záložní připojení nemají.
* Komunikace na záložních připojeních musí být chráněna proti neautorizovanému odposlechnutí a monitorování (např. prostřednictvím VPN, HW/SW šifrátory apod.). Zařízení pro připojení k CMS2 přes KIVS musí být pro tento účel vybavena.

## Připojení do Internetu

Operační střediska NIS IZS mohou mít přístup do Internetu. **Zřízení přístupu do Internetu není součástí projektu NIS IZS**. Doporučeným způsobem pro přístup do Internetu (a sTESTA) je využít služeb CMS2. Jednotlivé složky IZS mohou každá za sebe požádat provozovatele CMS2 o zřízení přístupu do Internetu, případně do sTESTA. Půjde o žádost na zřízení standardních služeb CMS2. Zejména o službu „Bezpečné připojení do Internetu“. Tato služba bude nabízet zabezpečené připojení do Internetu.

Poskytovatelem připojení bude provozovatel ITS v roli nekomerčního poskytovatele připojení k CMS2. Jednotlivé složky IZS použijí pro přístup do Internetu jim přidělené datové VPN NIS (technicky jde o VPN sítě ITS), tedy např. HZS použije VPN „HZS\_data“. KDC a DC použijí sběrnou VPN „NSPTV\_data“.

Na následujícím obrázku je schematicky znázorněno připojení HZS, PČR, ZZS, KDC NIS a DC NIS do Internetu a sTESTA přes CMS2. Orientace šipek udává směr navazování spojení, tj. od komponent NIS směrem do Internetu, respektive sTESTA.



## Řízení privilegovaného přístupu k systému

Přístup administrátorů a správců systému NIS IZS bude řízen. Budou vytvořeny postupy pro získání, využívání a odebrání privilegovaného přístupu k systému. Budou naplněny minimálně následující bezpečnostní požadavky:

1. Privilegovaný přístup k NIS ISZ budou mít jen odpovědní administrátoři.
2. Pravomoci jednotlivých administrátorů budou odděleny podle SoD (Segregation of Duties, oddělení odpovědností).
3. Budou prováděny kontroly, že práva přidělená pracovníků nejsou v rozporu s bezpečnostní politikou a odpovídají jejich pracovní náplni.
4. Budou rušena přístupová práva pracovníkům měnícím pozici nebo opouštějícím organizaci.
5. Je vedena kompletní evidence administrátorů a přidělených privilegií.
6. Kopie hesel účtů systémových správců budou bezpečně uloženy.
7. Použití privilegovaných účtů administrátorů bude minimální a účty nebudou používány k běžné práci v systému.

## Řízení změn v systému

Pro bezpečné řízení změn budou aplikována následující opatření:

1. Všechny změny v systému budou řízeny předem připraveným procesem.
2. Všechny změny budou před realizací schváleny oprávněným pracovníkem, dokumentovány a předem otestovány v testovacím prostředí, že změny nemají vliv na bezpečnost.
3. Jsou identifikovány všechny komponenty a oblasti, které změna ovlivní.
4. Jsou předem určeny osoby/role, které jsou odpovědné za změny.
5. Změny s vlivem na bezpečnostní požadavky jsou schvalovány vlastníkem aktiva systému, kterého se změna dotkne.
6. Změny budou v rámci možností realizovány v časech s nejnižší úrovní provozu.
7. Dodavatel nebude žádné aktualizace standardního software aplikovat na serverech a zařízeních automaticky, ale půjde vždy o manuální a kontrolovaný zásah.
8. Při aplikaci opravných balíčků bude Dodavatel dodržovat zásady (s výjimkou situací, kdy nutnost aplikace balíčků bude kritická, např. kvůli vysokému ohrožení NIS IZS existující zranitelností):
   1. Centrální systémy NIS IZS budou umístěny ve třech různých DC. Dodavatel aplikuje balíčky nejprve v DC3 a teprve po vyzkoušení v DC3 postupně s časovým odstupem na stejná zařízení v DC1 a DC2. Odstup bude zvolen podle typu zařízení, typu opravy a míře ohrožení existující zranitelnosti.
   2. Pro zařízení, která jsou v jedné lokalitě zdvojena, Dodavatel aplikuje balíčky postupně vždy nejprve na jedno a potom na druhé zařízení, pokud bude tento postup technicky možný. Odstup bude zvolen podle typu zařízení, typu opravy a míře ohrožení existující zranitelnosti.
   3. Dodavatel aplikuje najednou omezenou množinu oprav, aby byla usnadněna analýza případných problémů.
9. Pro řešení problémových stavů bude Dodavatel používat některý z následujících postupů, nebo jejich kombinace.
   1. Návrat k předcházející verzi software (tj. odstranění balíčku).
   2. Aktivace jiného zařízení jako náhrady.
   3. Omezení funkcionality zařízení, pokud se omezení nevztahuje na kritické funkce zařízení.
10. Všechny nouzové změny budou zaznamenány v registru změn a budou následně detailně zdůvodněny.
11. V pravidelných intervalech je prováděna kontrola registru změn pro zajištění, aby všechny žádosti o změnu byly řádně dokumentovány.

## Správa systému

Pro bezpečnou správu systému (HW i SW) budou aplikována následující opatření:

1. Správu NIS IZS bude provádět pouze autorizovaný personál Dodavatele.
2. Bude vedena evidence všech prací při správě NIS IZS. Všechny práce v rámci správy systému budou zdokumentovány.
3. Během provádění správy NIS IZS je uživatelům umožněno používání systému.
4. Plánované údržby nebudou zasahovat do ostrého provozu NIS IZS.
5. Fyzický i logický přístup pracovníků provádějících správu NIS IZS bude řízen, dokumentován a kontrolován. Budou vypracovány postupy pro řízení přístupu.
6. Nepoužívané zařízení NIS IZS bude fyzicky chráněno (bezpečně uskladněno).

## Řízení kontinuity a obnova po havárii

Detailní požadavky a návrh řešení pro oblast BCM a DRP jsou uvedeny v kapitole G. Výpočet spolehlivosti tohoto prováděcího konceptu. Z pohledu bezpečnosti musí být Dodavatelem naplněny minimálně následující požadavky:

1. Pro NIS IZS budou vytvořeny plány kontinuity systému a postupy obnovení činností. Budou vypracovány plány krizového řízení.
2. Strategie řízení kontinuity činností bude vytvořena na základě analýzy dopadů a hodnocení rizik. Jsou identifikována rizika, která mohou způsobit narušení chodu organizace
3. Plány a postupy budou identifikovat zapojení jednotlivých osob a jejich odpovědností. Budou dokumentovány role a odpovědnosti osob a týmů mající pravomoci během a po incidentu.
4. Postupy a plány budou přezkoumávány a aktualizovány při významných změnách v procesech nebo technologií NIS IZS a vždy, když se odhalí nedostatky.
5. Všechny nouzové postupy a procesy budou dokumentovány, aby mohly být později vyhodnoceny.
6. Všichni pracovníci Zadavatele i Dodavatele budou seznámeni s postupy a procesy pro případ stavu nouze a budou pravidelně školeni v oblastech BCM a DRP.
7. Opatření BCM a DRP budou přezkoumávána pomocí procesů testování, auditu i sebehodnocení, aby bylo zajištěno, že jsou přiměřená, vhodná a účinná. Nezávislé interní a externí audity BCM a DRP systému NIS IZS jsou prováděny odborně způsobilými osobami.

# Kybernetická bezpečnost NIS IZS

## Bezpečnostní monitoring NIS IZS

Bezpečnostní monitoring zajistí Dodavatel. Bezpečnostní monitoring splní následující požadavky.

1. Hlášení o výskytu bezpečnostních událostí v reálném čase.
2. Možnost vyhodnocování údajů o provozu NIS IZS od všech komponent. To znamená, že produkt bude umět přijímat a zpracovávat data v těch formátech, ve kterých je produkují jednotlivé systémy a zařízení NIS IZS. Bude podporovat sběr dat pomocí standardních protokolů, které se pro tento účel používají (zejména syslog, SNMP, netflow, a WMI).
3. Vyhodnocování bezpečnostních událostí za zvolené období.
4. Vytváření standardních a příležitostných reportů.

Bude vytvořen registr bezpečnostních metrik a pravidel, na jehož základě budou vyhodnocovány události a budou nastaveny postupy pro řešení alertů a incidentů. Množina událostí, o kterých bude systém informovat pomocí alertů v reálném čase, bude minimálně zahrnovat následující bezpečnostní události:

1. Pokus o útok proti NIS IZS. Jde o události zaznamenané aktivními síťovými prvky, firewally, servery a aplikací v tom rozsahu, v jakém jsou tyto komponenty schopné útoky detekovat. Zahrnuje pokusy o (D)DOS útok, výskyt malware, výskyt nebezpečných anomálií v síťových protokolech použitých pro komunikaci mezi prvky NIS IZS.
2. Pokus o nahrazení nějaké pracovní stanice nebo telefonu na operačních střediscích NIS IZS nepovoleným zařízením. Bude detekovat centrální NIS IPL. NIS IPL bude kontaktovat pracovní stanice a telefony a bude od nich vyžadovat zprávy. Pokud zařízení, které je dostupné pod IP adresou telefonu, respektive pracovní stanice, nepošle správnou odpověď, jde o bezpečnostní událost.
3. Pokus o neoprávněné připojení zařízení do sítě NIS IZS. Půjde o detekci připojení zařízení k aktivním síťovým prvkům, které jsou součástí infrastruktury NIS IZS. Nepoužívané porty aktivních prvků budou deaktivovány. Aktivní síťové prvky budou nakonfigurovány tak, aby hlásily změnu stavu jakéhokoli portu „down“ –> „up“ i opačně. Bezpečnostní dohledový systém bude vyhodnocovat, zda jde o zapnutí zařízení na povoleném portu, nebo o připojení zařízení k portu, který by neměl být aktivní.
4. Změny přiřazení hardwarových adres síťových karet a jejich logických adres zařízení, která jsou součástí NIS IZS. Bude detekována změna přiřazení IP adres a MAC adres. Změna jejich přiřazení signalizuje, že buď LAN rozhraní nějakého zařízení byla DHCP serverem přiřazena nová adresa, nebo v zařízení byla vyměněna LAN karta, nebo že se někdo pokouší falšovat svoji totožnost. Předpokládá se, že IP adresy budou zařízením NIS IZS přidělovány staticky. V případě virtuálního prostředí dochází v některých případech k přirozené změně MAC adres virtuálních serverů, např. v případě migrace virtuálního serveru mezi fyzickými servery. Tyto situace budou ze sledování vyloučeny, aby nedocházelo k false positives.
5. Pokus o změnu času některého zařízení NIS IZS. Jakýkoli pokus o změnu času zařízení NIS IZS může signalizovat pokus o narušení bezpečnosti NIS IZS. Správné nastavení času je podstatné při analýze bezpečnostních událostí, při některých metodách autentizace (certifikáty a bezpečnostní kalkulátory) a z hlediska důvěryhodnosti systémových a auditních záznamů.
6. Neúspěšný pokus o přístup k aktivnímu síťovému prvku NIS IZS. Jde o pokus o přihlášení, při kterém byl překročen maximální počet povolených neúspěšných pokusů.
7. Pokus o manipulaci s lokálním uživatelským účtem, nebo lokální uživatelskou skupinou na serveru NIS IZS. Týká se vytvoření, zrušení a změny účtu nebo skupiny. Jde o událost, ať byla operace úspěšná nebo ne a ať se jednalo o oprávněnou nebo neoprávněnou operaci. Předpokládá se, že lokální účty budou sloužit téměř výhradně pro servisní účely. Budou vytvořeny při instalaci NIS IZS a jejich změna bude výjimečná.
8. Neočekávaná aktivita pracovních stanic spojená s monitorováním prostředí, pokusy o distribuci malware nebo s únikem dat. Základní informace pro tuto analýzu je export netflow dat ze směrovačů.

Aby bylo možné požadované události sledovat, budou mít jednotlivé komponenty NIS IZS zapnuté logování a zapnutý auditing. Komponentami NIS IZS jsou zejména aktivní síťové prvky, aplikační servery a infrastruktura pro správu NIS IZS. Tím bude zajištěno, že vzniknou primární data o událostech podstatných z hlediska bezpečnosti přímo u zdroje. Tato data budou systémem bezpečnostního dohledu centralizována a centrálně vyhodnocována, oznamována (alerty) a prezentována.

Systém bezpečnostního dohledu (SIEM) bude upozorňovat na výskyt bezpečnostních událostí v reálném čase. Bude umožněno okamžité vyhodnocení událostí. Součástí bude uchování a archivace bezpečnostních záznamů pro potřeby dodatečných analýz a vyšetřování. Dodavatel bude tato data pravidelně vyhodnocovat a na základě vyhodnocení bude případně přijímat dodatečná bezpečnostní opatření a kontrolovat účinnost existujících opatření.

Systém bezpečnostního dohledu (SIEM) a systém pro zaznamenávání systémových událostí (log management) bude naplňovat minimálně následující požadavky:

* 1. Rozsah zaznamenávaných dat (logů) bude nastavitelný a budou zaznamenány všechny informace o události dle registru metrik a pravidel.
  2. Logy a záznamy budou bezpečně uloženy a archivovány. Vybrané záznamy budou archivovány minimálně po dobu 5 let.
  3. Nearchivované logy a záznamy budou bezpečně ničeny v rámci předem ustaveného procesu.
  4. Řízení přístupu k logům a záznamům bude přísně řízen. Viz kap. Řízení privilegovaného přístupu k systému.
  5. Všechny zaznamenávané události budou auditovatelné v souladu s registrem bezpečnostních metrik a pravidel. SIEM bude poskytovat nástroje pro práci s logy a záznamy. Prací je myšlené vyhledávání, filtrování, zobrazení detailu o auditním záznamu apod. Budou existovat prostředky pro analýzu logů a záznamů, které umožňují exportování do databázových a textových formátů.
  6. Systémy SIEM a log management budou napojeny na všechna zařízení a aplikace NIS IZS.
  7. V registru metrik a pravidel budou definovány události, které budou eskalovány dále k řešení v rámci procesu řízení incidentů. Budou vyšetřovány všechny podezřelé incidenty a zjištěné pokusy o narušení bezpečnosti.

## Ochrana proti virům a škodlivému kódu

Bude implementován systém na ochranu proti virům a škodlivému kódu. Bude specifikován rozsah implementace, tzn. zařízení, na kterých bude systém instalován. Systém bude udržován aktuální.

## Analýza technických zranitelností

Bude implementován proces pro řízení technických zranitelností, který zajistí, že každá identifikovaná zranitelnosti bude řádně řešena. Bude implementován systém pro analýzu technických zranitelností, který bude naplňovat minimálně následující požadavky:

1. Systém pro analýzu technických zranitelností bude napojen na všechna zařízení NIS IZS, aby se zjistilo, že všechna zranitelná místa a slabiny budou identifikovány a řešeny.
2. Bude kontrolována konfigurace síťových zranitelností, zda neobsahuje zranitelná místa.
3. Konfigurace síťových zařízení bude ověřována za použití specializovaných nástrojů.
4. Databáze známých zranitelností bude pravidelně aktualizována v minimálních intervalech.
5. Pro řízení a správu technických zranitelností budou určeny role a odpovědnosti.

## Zálohování a archivace

Zálohování je popsáno v kap. 1.4. části A - HW PKv51 a archivace v kap. 1.3. části A - HW PKv51. Budou naplněny základní bezpečností požadavky na zálohování:

1. Veškeré servery, data a datová pole budou zrcadlena na záložní úložiště v jiném DC.
2. Budou vytvořeny zálohy všech klíčových dat.
3. Zálohy dat budou chráněny stejně jako ostrá data
4. Bude udržována více než jedna generace záloh.
5. Budou pravidelně testovány postupy zálohování a obnovování záloh.
6. Zálohy budou zahrnovat i programové vybavení všech aplikací.
7. Určená data budou zálohována a archivována vhodnou technologií.
8. Dodavatelem budou vytvořeny postupy pro zálohování, archivaci a zničení dat.

# Personální a organizační bezpečnost

Bude zajištěna jasná definice kompetencí, práv a odpovědností jednotlivých rolí v systému na straně Zadavatele i Dodavatele. Obsazení všech rolí bude dokumentováno a udržováno aktuální.

Důležitým prvkem pro zajištění bezpečného provozu NIS IZS je dostatek kvalifikovaného a důvěryhodného personálu. Existují osoby, které budou mít fyzický přístup k zařízením NIS IZS, a osoby, které budou mít privilegovaný (ve smyslu vysokých oprávnění) logický přístup k zařízením NIS IZS.

Dodavatel si je vědom rizik spojených s fyzickým přístupem a logickým privilegovaným přístupem osob k zařízením NIS IZS a věnuje proto pozornost výběru osob na příslušné pozice. Nábor pracovníků se řídí interními pravidly Dodavatele. Na všech pozicích je požadován čistý trestní rejstřík a na výše uvedené pozice je požadována odpovídající kvalifikace, provádí se kontrola životopisu a zjišťují reference. S pracovníky je uzavírána dohoda o mlčenlivosti.

Pracovníci, kteří se budou podílet na zajištění provozu NIS IZS, mají odpovídající vzdělání a praxi. Dodavatel organizuje interní školení zaměstnanců v informační bezpečnosti a podle potřeby vysílá pracovníky na školení a kursy.

Dodavatel zajistí obsazení rolí správců NIS (role viz část „I - Školení“) kvalifikovanými a důvěryhodnými osobami. Jde o osoby, které provádějí administraci, monitoring, dohledování a podporu 1. a 2. úrovně celého systému NIS IZS.

## Personální bezpečnost

V rámci personální bezpečnosti budou naplněny minimálně následující požadavky:

1. Pro správu systému bude vytvořen dedikovaný tým po celou dobu využití systému.
2. Bude připraveno úvodní školení pro pracovníky pracující s informacemi a daty NIS IZS.
3. Budou stanoveny postihy, které hrozí zaměstnancům při zanedbání bezpečnostních požadavků.
4. Všechny osoby se vztahem k NIS IZS musí podepsat závazek o zachování mlčenlivosti, pokud pro ně požadavek mlčelivosti nevyplývá přímo ze zákona nebo z pracovně právního vztahu.
5. Bude stanovena strategie bezpečnostního vzdělávání a školení pro práci s NIS IZS (pro pracovníky Dodavatele i Zadavatele).
6. Bude provedeno školení všech pracovníků pro práci s NIS IZS, které bude přizpůsobeno roli, odpovědnostem a schopnostem dotyčné osoby.
7. Je vytvořena a udržována evidence zaměstnanců, kteří se zúčastnili školení pro práci s NIS IZS.

## Organizace bezpečnosti

Bezpečnost NIS IZS bude organizačně řízena ze strany Dodavatel tak, aby byla vždy a za všech okolností zajištěna požadovaná úroveň bezpečnosti systému. Budou naplněny minimálně následující požadavky:

1. Za bezpečnostní činnosti v rámci NIS IZS budou stanoveny konkrétní role a odpovědnosti
2. Budou určeni pracovníci odpovědní za přezkoumání/audit stavu bezpečnosti NIS IZS.

## Řízení bezpečnostních incidentů

Budou ustaveny postupy pro řízení bezpečnostních incidentů, které budou naplňovat minimálně následující požadavky:

1. Budou vytvořeny a zavedeny postupy pro řízení bezpečnostních incidentů, včetně schéma pro hlášení incidentů a podezření.
2. Budou vypracovány pracovní postupy pro řešení incidentů.
3. Incidenty budou hlášeny schváleným způsobem.
4. Bezpečnostní incidenty budou zaznamenány v souladu se zavedenými postupy pro hlášení incidentů.
5. Všechny slabiny bezpečnosti budou bez prodlení ohlašovány.
6. Pracovníci NIS IZS nebudou sami odstraňovat vzniklé problémy, pokud k tomu nebudou odpovědnou osobou přímo vyzváni.
7. Budou zavedeny mechanismy a nástroje pro analýzu incidentu.
8. Budou shromažďovány důkazy na podporu kroků proti osobám či organizacím.
9. Budou vyšetřovány všechny podezřelé incidenty a zjištěné pokusy o narušení bezpečnosti.
10. Vyšetřování bude prováděno odpovědnými pracovníky Dodavatele v rozsahu jeho kompetence. Zadavatel poskytne při vyšetřování bezpečnostních incidentů požadovanou součinnost.
11. Po skončení vyšetřování bude vypracovávána zpráva pro vedení Zadavatele i Dodavatele, která bude popisovat příčiny, škody a provedené nápravné činnosti.

# Testování bezpečnosti NIS IZS

Před zahájením provozu a následně pravidelně v průběhu používání NIS IZS budou prováděny sady bezpečnostních testů, které jsou v základu specifikovány v následujících kapitolách. Pro provádění testů budou stanoveny a naplněny následující požadavky:

1. Budou vytvořeny plány bezpečnostního testování před a po uvedení NIS IZS do provozu.
2. Pro testování bezpečnosti NIS IZS jsou vytvořena akceptační kritéria.
3. Budou stanoveny výkonnostní a kapacitní požadavky na bezpečnost systému.
4. Testy budou zahrnovat testování bezpečnostních funkcí.
5. Budou stanoveny testy, data potřebná pro testy a odhadnuty výsledky testů.
6. Závěry testů budou rozděleny podle závažnosti.
7. Testování bude prováděno podle sady standardních bezpečnostních testů.
8. Testy budou sestaveny mj. na základě znalosti slabin systému.
9. Bezpečnostní testy budou kontrolovat prosazení bezpečnostních požadavků podle akceptačních kritérií.
10. Bude prováděna kontinuální kontrola, zda jsou v systému aktivovány bezpečnostní funkce stanovené systémovou bezpečnostní politikou NIS IZS.
11. Bezpečnostní testy budou prováděny i po celou dobu vývoje systému.

## Testování bezpečnosti aplikací

Preventivním prostředkem pro zajištění bezpečnosti aplikací vyvíjených vlastními silami Dodavatele bude statické testování kódu. Vyvíjené programy i programy přebírané z externích zdrojů ve zdrojovém tvaru budou testovány analyzátory zdrojových programů s cílem odhalit případné zranitelnosti v programech a odstranit je před nasazením aplikací do provozu. Týká se aplikací:

* Aplikace NSPTV.
* Aplikace TEL (telefonie).
* Aplikace REC (nahrávání).
* Centrální integrační platforma.
* Krajské integrační platformy.
* Centrální GIS.
* Krajské GIS.

Statické testování aplikací bude doplněno dynamickým testováním, které bude primárně orientováno na odolnost vůči chybám ve vstupních datech. Speciálně bude provedeno testování aplikací v následujících situacích.

* Chybějící geografická data. Aplikace je nebude mít z nějakého důvodu dostupná.
* Chyba v geografických datech. Špatný formát dat, neúplná data, pozměněná data.
* Chyba v datech posílaných z příjmu tísňového volání v DC na krajská operační střediska. Špatný formát dat, neúplná data.
* Chyba v datech posílaných z krajských operačních středisek na integrační platformu.
* Logicky nekonzistentní data posílaná přes integrační platformu.
* Chybějící lokalizační údaje o přijatém tísňovém volání.
* Chyba v lokalizačních údajích o přijatém tísňovém volání. Pozměněná data, např. nesmyslné souřadnice.
* Nedostupné úložiště pro ukládání záznamů o přijatých tísňových voláních.
* Nedostupné údaje o dopravní situaci.
* Chyba v datech o dopravní situaci.
* Nedostupné údaje o meteorologické situaci.
* Chyba v datech o meteorologické situaci.

Dodavatel provede statické i dynamické testování před nasazením aplikací do provozu. Dynamické testování provede na produkčním prostředí (ale před nasazením aplikací do provozu).

Po nasazení do provozu provede Dodavatel statickou analýzu příslušné části zdrojového kódu po větších změnách v některé aplikaci a při stejné příležitosti provede relevantní dynamické testy.

Po nasazení do provozu bude Dodavatel provádět dynamické testy pouze v testovacím nebo vývojovém prostředí.

## Testování bezpečnosti infrastruktury

**Před nasazením NIS IZS do provozu** Dodavatel provede bezpečnostní testy infrastruktury NIS IZS na produkčním prostředí.

* Testy filtrace provozu v operačních střediscích.
  + Test: z VPN HZS\_data zkusit navázat spojení s centrálním NIS IPL protokolem telnet.

Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.

* + Test: z VPN HZS\_data zkusit navázat spojení na nějakou adresu ve VPN PCR\_protokolem HTTP.

Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.

* + Test: z VPN\_HZS poslat ICMP time stamp na adresu v téže VPN v jiném kraji.

Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.

* + Test: z VPN\_HZS poslat pakety s nastavenými IP options na adresu v téže VPN v jiném kraji.

Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.

* + Test: z VPN\_HZS poslat pakety se  zdrojovými IP adresami z VPN\_PCR do VPN\_PCR.

Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.

* + Test: z VPN\_HZS poslat pakety s nastaveným source routing na adresu v téže VPN v jiném kraji.

Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.

* + Test: z VPN\_HZS poslat broadcast pakety, ve kterých je cílovou IP sítí (subnet) stejná VPN.

Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.

* + Test: na operačním středisku HZS zablokovat přístup z i do VPN PCR\_data a vyzkoušet komunikaci s PČR přes integrační platformu, standardně jde o povolený provoz. Po testu přístup opět odblokovat.

Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.

* Testy ochrany CE směrovačů v operačních střediscích.
  + Test: zadat při přihlašování k CE směrovači nesprávné heslo o jednu vícekrát, než je povolený počet neúspěšných pokusů, potom zadat správné heslo, cílem je vyzkoušet zamykání účtů po neúspěšných pokusech o přístup k CE směrovači.

Očekávaný výsledek: CE směrovač připojení odmítne i při zadání správného hesla a v logu routeru se objeví záznam o odmítnutí.

* + Test: zadat při přihlašování k CE směrovači nějaké standardní předdefinované jméno.

Očekávaný výsledek: CE směrovači připojení odmítne a v bezpečnostním monitoringu se objeví záznam o odmítnutí.

* + Test: zadat při přihlašování k CE směrovači nějaké jméno, které není mezi jmény s povoleným přístupem.

Očekávaný výsledek: CE směrovač připojení odmítne a v bezpečnostním monitoringu se objeví záznam o odmítnutí.

* + Test: zablokovat přístup CE směrovače k AAA serveru a zadat při přihlašování k CE směrovači lokální účet a správné heslo a potom nelokální účet a správné heslo.

Očekávaný výsledek: CE směrovač připojení pro lokální účet akceptuje a pro nelokální odmítne a odmítnutí zaznamená v bezpečnostním monitoringu.

* + Test: přihlásit se k CE směrovači s použitím platného jména a hesla a počkat na automatické odhlášení.

Očekávaný výsledek: uživatel je automaticky odhlášen.

* + Test: pokusit se k CE směrovači přihlásit s použitím protokolu telnet.

Očekávaný výsledek: CE směrovač nereaguje, neobjeví se výzva k zadání jména a hesla.

* + Test: pokusit se k CE směrovači přihlásit z počítače, jehož IP adresa není mezi povolenými.

Očekávaný výsledek: CE směrovač nereaguje, neobjeví se výzva k zadání jména a hesla.

* + Test: provést skenování portů proti CE směrovači, zjistit dostupné síťové služby.

Očekávaný výsledek: Podaří se zjistit pouze čísla portů.

* Test: pokusit se o SNMP přístup k CE směrovači z počítače, jehož IP adresa není mezi povolenými.

Očekávaný výsledek: CE směrovač nereaguje, není možné získat žádné informace.

* Test: pokusit se o SNMP přístup k CE směrovači s použitím standardních implicitních community strings.

Očekávaný výsledek: CE směrovač nereaguje, není možné získat žádné informace.

* Test: provést základní útoky proti operačnímu systému CE směrovači s využitím útoků předdefinovaných v použitém nástroji, lze použít freeware nástroje (Nexpose Community edition, Nessus, OpenVAS).

Očekávaný výsledek: není nalezena žádná závažná zranitelnost.

* Test: provést DOS útok proti CE směrovači a v době útoku se k němu přihlásit přes správcovské rozhraní.

Očekávaný výsledek: k CE směrovač je možné se přihlásit i během útoku.

* Testy připojení neschváleného zařízení.
  + Test: připojit notebook k neaktivnímu portu síťového prvku a zkusit kontaktovat centrální nebo krajský NIS.

Očekávaný výsledek: spojení s NIS se nenaváže.

* + Test: připojit notebook k aktivnímu portu síťového prvku (odpojit nějakou pracovní stanici) a zkusit http na centrální nebo krajský NIS, cílem je pokusit se obejít autentizaci zařízení připojených k aktivním síťovým prvkům.

Očekávaný výsledek: spojení s NIS se nenaváže a v bezpečnostním monitoringu se objeví záznam o pokusu.

* + Test: připojit notebook k aktivnímu portu síťového prvku (odpojit nějakou pracovní stanici) a počkat, cílem je otestovat kontrolu připojených zařízení.

Očekávaný výsledek: v bezpečnostním monitoringu se objeví záznam o připojení neznámého zařízení.

* + Test: připojit k povolenému síťovému portu aktivního síťového prvku rozbočovač (hub) a k němu autentizovanou pracovní stanici a notebook a zkusit z notebooku kontaktovat centrální nebo krajský NIS.

Očekávaný výsledek: spojení s NIS se nenaváže a v bezpečnostním monitoringu se objeví záznam o pokusu.

* Simulace výpadku ITS a aktivace náhradních komunikačních linek.

**Po nasazení NIS do provozu** Dodavatel zopakuje relevantní bezpečnostní testy v testovacím nebo vývojovém prostředí NIS IZS vždy před provedením změn konfigurace komponent v produkčním prostředí.

## Kontroly souladu

Systém musí procházet pravidelnými audity a kontrolami, jejímž sponzorem může být Zadavatel i Dodavatel. Audity budou naplňovat následující požadavky:

1. Splnění bezpečnostních požadavků a standardů je ověřováno Dodavatelem a nezávislou třetí stranou. Aby byl zajištěn soulad mezi fyzickými, procedurálními a technickými protiopatřeními, jsou prováděny nezávislou osobou pravidelně bezpečnostní analýzy.
2. Bezpečnostní audity jsou prováděny podle předem schváleného plánu, který je revidován minimálně jednou ročně.
3. Výsledky bezpečnostního auditu jsou předkládány vedení Zadavatele i Dodavatele.
4. Jsou prováděny pravidelné i namátkové kontroly souladu faktického nastavení s bezpečnostními předpisy.
5. Jsou explicitně určeny a zdokumentovány veškeré požadavky odpovídající zákonům, nařízením a smlouvám a tyto jsou pravidelně kontrolovány.
6. Je pravidelně prováděn audit nainstalovaného programového vybavení na zařízeních NIS IZS a jsou realizována nápravná opatření v případě auditních nálezů. Jsou implementována řešení zajišťující nepřekročení limitu stanoveného licencí.
7. Jsou udržovány registry/seznamy všech aktiv/zařízení NIS IZS a je pravidelně prováděn soulad reálného stavu systému s registry.

# Bezpečnostní dokumentace pro provoz

Pro NIS IZS bude vytvořena bezpečnostní dokumentace, která bude zahrnovat všechny bezpečnostní požadavky na vývoj, implementaci a provoz systému, včetně přesných určení rolí a odpovědností. Základní struktura bezpečnostní dokumentace NIS IZS bude následující:

1. Systémová bezpečnostní politika NIS IZS
2. Bezpečnostní směrnice/Administrátorský manuál NIS IZS
3. Bezpečnostní směrnice/Uživatelský manuál NIS IZS
4. Směrnice pro řízení bezpečnostních incidentů NIS IZS
5. Plány kontinuity a obnovy NIS IZS
6. Bezpečnostní postupy pro administrátory a uživatele (podřízení Administrátorskému a Uživatelskému manuálu)

# Příloha

## Rejstřík

[Model 1: Rozsah NIS IZS 6](#_Toc364702015)

[Model 2: Připojení zařízení v KDC 18](#_Toc364702016)