**Standardy IS VZP – NIS**

**UPOZORNĚNÍ:**

Tento dokument je zpracován Všeobecnou zdravotní pojišťovnou České republiky (dále též jen „VZP ČR“ nebo „VZP“). Všeobecná zdravotní pojišťovna České republiky jej uveřejňuje v rámci zadávací dokumentace jí zadávaných veřejných zakázek. Tento okument umožňuje utvořit si představu o standardech informační architektury ICT VZP ČR. Účelem jeho uveřejnění je poskytnout informace nezbytné pro integraci dodávané komponenty se stávajícím informačním systémem v souladu se Standardy ICT- VZP- NIS.

Uveřejněním tohoto dokumentu není dotčena právní odpovědnost spojená s jeho zneužitím.

V tomto dokumentu bylo použito názvů subjektů a názvů produktů, které mohou být chráněny příslušnými právními předpisy.

**Otevřením tohoto dokumentu berete výše uvedené skutečnosti na vědomí.**

**Verze dokumentu**

|  |  |  |  |
| --- | --- | --- | --- |
| **Verze**  | **Datum**  | **Autor**  | **Popis**  |
| 1.06  | 11.10.2017  | ÚICT VZP ČR  |   |

**Obsah**

[**2.1. Aplikační – obecné standardy 6**](#_Toc511642110)

[**2.1.1. Třídy Aplikací 6**](#_Toc511642111)

[**2.2. Integrační a komunikační standard 7**](#_Toc511642112)

[**2.2.1. Integrace se stávajícím IS 7**](#_Toc511642113)

[**2.3. Vývojové standardy 7**](#_Toc511642114)

[**2.3.1. Používané vývojové nástroje pro interní vývoj aplikací: 7**](#_Toc511642115)

[**2.3.2. Vývojová a testovací prostředí 7**](#_Toc511642116)

[**2.4. Testovací standardy 8**](#_Toc511642117)

[**2.5. Dokumentační standard 9**](#_Toc511642118)

[**3.1. HW 13**](#_Toc511642119)

[**3.2. Sítě 14**](#_Toc511642120)

[**3.2.1. Celkové schéma sítě VZP ČR 14**](#_Toc511642121)

[**3.2.2. LAN RP a KLIPRů 15**](#_Toc511642122)

[**3.2.3. Bezdrátová síť (WIFI) 16**](#_Toc511642123)

[**3.2.5. Datová centra On premise 16**](#_Toc511642124)

[**3.2.6. Perimetr 18**](#_Toc511642125)

[**3.2.7. Síťové služby 18**](#_Toc511642126)

[**3.2.8. Sjednocená komunikace 19**](#_Toc511642127)

[**3.3. OS 19**](#_Toc511642128)

[**3.3.1. OS pro aplikace třídy A 19**](#_Toc511642129)

[**3.3.2. OS pro aplikace třídy B 19**](#_Toc511642130)

[**3.3.3. Prostředí pro virtualizaci 19**](#_Toc511642131)

[**3.3.4. Požadavky na linuxové účty 20**](#_Toc511642132)

[**3.4. Middleware 20**](#_Toc511642133)

[**3.4.1. Integrační platforma 20**](#_Toc511642134)

[**3.4.2. Aplikační servery 21**](#_Toc511642135)

[**3.4.3. Webové servery 21**](#_Toc511642136)

[**3.5. Virtualizovaná infrastruktura pro hostování aplikací 21**](#_Toc511642137)

[**3.6. Deployment aplikací NIS do prostředí v DC 22**](#_Toc511642138)

[**3.7. Datové a databázové služby 22**](#_Toc511642139)

[**3.6. Koncová zařízení 24**](#_Toc511642140)

[**3.7. Elektronická pošta 25**](#_Toc511642141)

[**3.8. Active Directory 25**](#_Toc511642142)

[**3.9. PKI 26**](#_Toc511642143)

[**4.1. Dodržování legislativních požadavků 26**](#_Toc511642144)

[**4.2. Dodržování obecných standardů a doporučení 26**](#_Toc511642145)

[**4.3. Minimalizování běžících služeb 26**](#_Toc511642146)

[**4.4. Nevyhovující služby nebo protokoly 26**](#_Toc511642147)

[**4.5. Minimální požadavky na šifrovací algoritmy 27**](#_Toc511642148)

[**4.6. Mechanismus obrany proti hádání přístupu do systému 27**](#_Toc511642149)

[**4.7. Důvěrnost 27**](#_Toc511642150)

[**4.7.1. Klasifikační schéma informačních/datových aktiv 27**](#_Toc511642151)

[**4.7.2. Bezpečnost umístění informačních/datových aktiv/souborů 27**](#_Toc511642152)

[**4.7.3. Bezpečnost přenosu dat 28**](#_Toc511642153)

[**4.7.4. Popis umístění dat a jejich životní cyklus 28**](#_Toc511642154)

[**4.8. Kompatibilita s DR (Disaster Recovery) 29**](#_Toc511642155)

[**4.9. Integrita dat 29**](#_Toc511642156)

[**4.10. Nepopiratelnost 29**](#_Toc511642157)

[**4.10.1. Obecné požadavky na auditing/logování 29**](#_Toc511642158)

[**4.10.2. Aplikační auditní log 30**](#_Toc511642159)

[**4.10.3. Nástroje auditu/logování 31**](#_Toc511642160)

[**4.10.4. Požadavky na ověření a sledování identity uživatele IS 31**](#_Toc511642161)

[**4.10.5. Přístupová práva uživatelů IS 31**](#_Toc511642162)

[**4.11. Penetrační testy 32**](#_Toc511642163)

[**5.1. Monitoring 32**](#_Toc511642164)

[**5.1.1. Rozsah monitoringu 32**](#_Toc511642165)

[**5.1.2. Používané dohledové nástroje pro On premise řešení 32**](#_Toc511642166)

[**5.1.3. Požadavky na procesy z hlediska monitoringu 33**](#_Toc511642167)

[**5.1.4. Požadavky na návrh monitoringu 33**](#_Toc511642168)

[**5.1.5. Požadavky na rozhraní pro monitoring 33**](#_Toc511642169)

[**5.2. Zálohování a archivace 34**](#_Toc511642170)

[**5.2.1. Zálohovací systém 34**](#_Toc511642171)

[**5.2.2. Požadavky na aplikační celky z pohledu jejich zálohování: 35**](#_Toc511642172)

[**5.3. Definice provozních parametrů služby/aplikace (SLA) 35**](#_Toc511642173)

[**5.4. Podmínky převzetí do rutinního prostředí a aplikační podpory 36**](#_Toc511642174)

[**5.5. Vazba na ITIL procesy 37**](#_Toc511642175)

[**5.5.1. Definování veškerých eskalačních procedur u aplikace - správa HelpDesku/ServiceDesku 37**](#_Toc511642176)

[**5.5.2. Zavedení aplikace do incident managementu 37**](#_Toc511642177)

[**5.5.3. Zavedení aplikace pod standardní řízení změn - change management 37**](#_Toc511642178)

[**5.5.4. Zavedení aplikace do release plánů - release management 37**](#_Toc511642179)

[**7. Výjimky ze standardu: 38**](#_Toc511642180)

[**7.1. Integrace se stávajícím IS 38**](#_Toc511642181)

* 1. **Úvod**

**STANDARDY IS VZP - NIS**

* + - **Představují -** soubor pravidel určených pro vytváření, rozvoj a využívaní IS VZP ČR.

* + - **Obsahují -** charakteristiky, metody, postupy a podmínky, zejména pokud jde o bezpečnost a integrovatelnost s jinými informačními komponenty a systémy.

* + - **Jsou určeny -** pro všechny dodavatele řešení/služeb/komponent jako pravidla dodávek IS/IT a k vývoji aplikací a jejich releasů.

* + - **Všichni dodavatelé komponent IS do VZP** jsou povinni po akceptaci standardu ho respektovat ve znění, v jakém ho přijali.

* + - **Od standardu se lze odchýlit pouze na základě výjimky** udělené vlastníkem standardu VZP ČR.

* + - **Při vydání nové verze standardu dodavatelé jsou vyzváni k přistoupení k nové verzi standardu** pro další dodávky. Pokud není poskytované řešení kompatibilní s novou verzí standardu, požádají VZP o výjimku.

* + - **Jejich účelem je** nasazení a následné provozování řešení/komponent v rutinním prostředí VZP s požadovanými garancemi, s požadovanými provozními parametry, s požadovanou odbornou aplikační a provozní podporou provozu IT při optimalizaci řešení IT.

* 1. **Architektonické a QA standardy**

## 2.1. Aplikační – obecné standardy

* Aplikace musí být navržena jako vícevrstvá a tyto vrstvy musí být jasně definovány a jejich rozdělení striktně dodržováno (např. presentační vrstva, vrstva business logiky, datová vrstva);
* Řešení je složeno z jednotlivých komponent s definovanými a oddělenými funkčnostmi bez duplicit a distribuované funkční logiky.
* Řešení by mělo být tvořeno ze sady relativně nezávislých modulů, aby změna v jednom z nich neznamenala (podstatný) zásah do zbývajících modulů
* Aplikace by měla mít deklarovatelným způsobem ošetřeny architektonické aspekty: škálovatelnost, flexibilita;
* Součástí návrhu řešení a realizace je požadován kapacitní a výkonnostní sizing systému s výhledem na 5 let.
* Aplikace musí splňovat požadavky popsané níže v kapitole „Zálohování“

###  2.1.1. Třídy Aplikací

#####  Třída A

Jedná se o business kritické a technologické aplikace, jejichž výpadek má zásadní charakter. Garantovaná dostupnost těchto aplikací je 99,4% v požadovaném režimu provozu (standardně 7x24 nebo 5x16).

Aplikace v této třídě pracují v režimu aktiv/pasiv mezi oběma lokalitami. Jsou provozované na infrastruktuře, která eliminuje dopady výpadků fyzických komponent HW. V případě výpadku celé primární lokality bude aplikace po dobu nutnou k přepnutí do záložní lokality dočasně nedostupná. Přepnutí může být provedeno buď automaticky, nebo poloautomaticky. V záložní lokalitě je připravena infrastruktura primárně využívána pro testovací prostředí, které bude v případě přepnutí produkčních aplikací omezeno, nebo vypnuto. Přepnutí do záložní lokality může mít vliv na výkonnost aplikace. Data jsou zrcadlena do záložní lokality prostřednictvím vhodné technologie.

#####  Třída B

Jedná se o aplikace, které nepatří mezi business kritické a mají nižší nároky na zajištění jejích dostupnosti. Požadovaná dostupnost je 98,1% v požadovaném režimu provozu 5x8 nebo 5x16. Aplikace nemusí být provozované na infrastruktuře, která eliminuje dopady výpadků fyzických komponent HW.

V případě nedostupnosti není počítáno s automatickým nebo poloautomatickým převodem do záložní lokality. Data nejsou zrcadlena do záložní lokality.

Veškeré nově implementované nebo upravované aplikace obou tříd musí umožňovat odklad dat a vytváření archivů a to jak z databázových objektů, tak z nedatabázových oblastí (z filesystémů).

## 2.2. Integrační a komunikační standard

* Veškeré vazby systému na ostatní systémy jsou formou volné vazby (loosely coupled), doporučeným mechanizmem jsou WS, JMS. Případně lze využívat souborový přenos.
* Vazby systému na ostatní systémy formou vazby (REST/JSON) jsou možné po schválení výjimky.
* Při implementaci nových rozhraní upřednostňovat webové služby.
* Spojení mezi systémy VZP provádět přes integrační platformu (ESB).
* V maximální možné míře je nutno využívat stávajících již implementovaných aplikačních služeb nabízených v infrastruktuře VZP.
* Komunikace je v zásadě asynchronní (synchronní pouze ve výjimečných odůvodněných případech);
* Komunikace musí být odolná proti výpadku jedné strany
* Komunikace by měla maximálně omezit využití způsobu distribuované transakce, dvoufázové potvrzení transakce (two-phase- commit);
* Není povoleno využívat integraci aplikací na úrovni databází (link mezi databázemi);
* V rámci aplikace musí být zajištěna kontrola vstupů a výstupů (formátů dat), automatické přenosy obsahují kontrolní součty a zabezpečení, manuální přenosy jsou nepřípustné;
* Proces zpracování dávek musí obsahovat dílčí kontrolní body a kontrolní mechanizmy.

###  2.2.1. Integrace se stávajícím IS

Ke dni vzniku tohoto standardu VZP provozuje stávající IS řízený historickou verzí standardu. Způsob integrace s tímto IS je proto prováděn odchylně od tohoto standardu. Tato výjimka je zachycena v kapitole 7.1 Integrace se stávajícím IS.

## 2.3. Vývojové standardy

### 2.3.1. Používané vývojové nástroje pro interní vývoj aplikací:

* Funkční analýza a design: Enterprise Architekt, MS Word, Balsamiq Mockups o Technický design-aplikační logika: Visual Studio 2015/2017
* Technický design-datový design: Visual Studio 2017 Database Tools (MSSQL / Oracle) o Technický design-integrační procesy: OpenAPI / AutoRest (Enterprise Architect, MS Word) o Správa verzí: Visual Studio Team Services (Git)
* Vývoj aplikací: Visual Studio 2015/2017, Visual Studio Code, SQL Server Management

Studio, XCode / Android Studio, SOAP UI, Postman o Migrace a deployment aplikací: Visual Studio Team Services

###  2.3.2. Vývojová a testovací prostředí

Vyvíjená aplikace musí mít definována minimálně prostředí: o izolované prostředí určené konkrétnímu vývojáři

* prostředí určené pro ověřovací test v rámci QA vývoje, preferováno nasazování na tato prostředí probíhá automaticky
* prostředí určené pro ověřovací a akceptační test garanty aplikací, nasazení na tato prostředí je řízeno manažerem UAT

## 2.4. Testovací standardy

* Součástí každého řešení/ komponenty je testovací dokumentace (viz dokumentační standard)
* Součástí každého řešení jsou provedené testy dle dokumentace příslušné aplikační komponenty
* Testování se provádí na anonymizovaných datech (součástí řešení jsou nástroje pro anonymizaci testovacích dat)

####  Typy požadovaných testů pro předání do provozu IT

|  |
| --- |
| **Vývojové testování - strana dodavatele**  |
| **Název testu**  | **Provádí**  | **Vstupy**  | **Výstupy**  |
| unit test  | vývojoví pracovníci a testeři dodavatele komponenty  | Návrh architektury testování Plán testů Testovací scénáře a testovací případy Specifikace testovacích dat Testovací data  | Odsouhlasené testovací scénáře a testovací případy Odsouhlasená specifikace testovacích dat Záznam výsledků testů Protokol o provedení vývojových testů  |
| assembly test  |
| funkční test  |
| test výjimek  |
| **Systémové testování - strana odběratele (VZP ČR)**  |
| **Název testu**  | **Provádí**  | **Vstupy**  | **Výstupy**  |
| smoke test  | testeři dodavatele komponenty společně s testery VZP ČR  | Testovací scénáře a testovací případy Specifikace testovacích dat Testovací data Protokol o provedení vývojových testů  | Odsouhlasené testovací scénáře a testovací případy Odsouhlasená specifikace testovacích dat Záznam o výsledku testů Protokol o provedení systémových testů  |
| funkční test  |
| test výjimek  |
| integrační test  |
| **Výkonnostní testy - strana odběratele (VZP ČR)**  |
| **Název testu**  | **Provádí**  | **Vstupy**  | **Výstupy**  |
| zátěžový test  | testeři VZP ČR  | Projektová dokumentace Plán testů Analýza pro výkonnostní test Testovací data Testovací scénáře Protokol o provedení systémových testů  | Výsledky výkonnostního testu Zpráva o výkonnostním testu  |
| stress test  |
| **Bezpečnostní testy**  |
| **Název testu**  | **Provádí**  | **Vstupy**  | **Výstupy**  |
| bezpečnostní test  | testeři OBIT VZP ČR  | Návrh architektury bezpečnostního testování Plán testů Testovací scénáře a testovací případy  | Zpráva o bezpečnostním testu Záznam výsledků testu  |
| Penetrační test  | testovací tým dodavatele nebo externí nezávislý dodavatel  | Návrh penetračního testu Plán testů Testovací scénáře a testovací případy  | Zpráva o penetračním testu Záznam výsledků testu  |
| **Akceptační uživatelské testy - strana odběratele (VZP ČR)**  |
| **Název testu**  | **Provádí**  | **Vstupy**  | **Výstupy**  |
| akceptační uživatelský test  | testeři VZP ČR  | Protokol o provedení systémových testů Testovací scénáře, testovací případy Data ze systémových testů   | Záznam výsledků testu Akceptační protokol za testování  |

## 2.5. Dokumentační standard

Dokumentace systému se skládá z:

* Celková – úplná dokumentace. Popisuje úplně systém v jeho aktuální podobě.
* Přírůstek dokumentace – dokumentace konkrétní změny provedené oproti celkové dokumentaci.

* Celková dokumentace k dodanému řešení musí být dodavatelem pravidelně aktualizovaná a to při významných změnách / velký release .
* Dokumentace musí být min. 1 x ročně konsolidována, všechny dílčí změny zapracovány do úplné verze a předány VZP.

* Kromě odůvodněných a schválených a smysluplných výjimek (např. zdrojový kód) je dokumentace vedena v nástroji Sparx Enterprise Architect.

Níže uvedený seznam dokumentů je volitelný. Dle předmětu specifikace zakázky na dodávku do IS VZP bude proveden výběr povinně požadovaných dokumentů od dodavatele řešení.

|  |  |  |
| --- | --- | --- |
| **Dokumentační oblast**  | **Podrobnější popis**  | **Dokumenty**  |
| Funkční dokumentace   | Funkční dokumentace definuje funkčnosti systému a jejich chování v souvislosti s řešením služeb pro podporu business procesu. Představuje detailní popis, jak software funguje, bez vazby na konkrétní technologii či detailní architekturu systému. Zabývá se proto business elementy, jako jsou: business entity, schopnosti, procesy, role, cíle, lokality a taky vnější omezení (např. legislativní) a jiné vlivy, které je třeba při návrhu řešení brát v potaz. Funkční a nefunkční požadavky na řešení jsou definovány v katalogu požadavků. Popis požadavku na změnu definuje klíčové potřeby uživatelů na IS, podporované procesy. Při velkých změnách obsahuje funkční dokumentace i návrh nového řešení a způsob, jak nového řešení dosáhnout ve vazbě na stávající stav.  | Katalog požadavků na dodané řešení do IS VZP Účastníci řešení Pojmy a artefakty řešení Statický model Doménový model Statický model Logická architektura Konceptuální datový model Procesy podporované dodaným řešením Dynamický model Funkční předpoklady, omezení Katalog služeb komponenty Postup implementace a migrace   |
| Technická dokumentace   | Technická dokumentace obsahuje návrh IT řešení business problémů specifikovaných na úrovni business analýzy a obsažené ve funkční dokumentaci. Navrhuje funkčnost jednotlivých technických komponent IT systémů, místo řešení požadavků v rámci vrstev nebo jiných částí IT architektury. Zpodrobňuje požadavky z funkční dokumentace na implementační úroveň. Obsahuje popis aplikační architektury, front end komponenty, validace, popis business logiky, orchestrace, popis datové vrstvy, deployment, konzumované služby IS, napojení na  | Aplikační architektura Integrační architektura Datová architektura Technologická architektura Technické předpoklady, omezení Postup implementace a migrace   |

|  |  |  |
| --- | --- | --- |
|  | integrační komponenty… Provádí přiřazení funkčních služeb do IT komponent / domén. Provádí přiřazení business objektů do IT komponent / domén. Při velkých změnách architektury (náhrady komponent) obsahuje návrh nového řešení a způsob, jak nového řešení dosáhnout ve vazbě na stávající stav.  |  |
| Bezpečnostní dokumentace  | Způsob řešení požadavků na bezpečnost systému.   | Autentizace Autorizace Monitoring provozní Monitoring bezpečnostní Zálohování a archivace Havarijní plánování  |
| Testovací dokumentace  | Dokumentuje průběh testování pro danou komponentu. Rozsah povinné dokumentace se stanoví dle metodiky testování VZP v závislosti na charakteru komponenty, typu vývoje a správy systému, včetně postupů pro obnovu dat, jak z produkčního prostředí, tak mezi testovacími prostředími. Dále bude dokumentace popisovat návrhy řezů dat a možnosti pseudonymizace a anonymizace.    | Testovací strategie Testovací plán Test scope - rozsah testů Testovací scénáře Testovací případy Testovací skripty Testovací data Záznam o provedení testu Postup na obnovu dat v testovacím prostředí Postup pro vytváření řezů dat a anonymizaci dat  Akceptační protokol  |
| Provozní dokumentace   | Provozní dokumentace potřebná k provozování a správě dodaného řešení v prostředí VZP.  | Zálohování a archivace, odklady dat, obnova dat – provozní příručka Monitoring – provozní příručka Administrátorská příručka Uživatelská příručka Instalační postup Konfigurační příručka Tabulky předávání do provozu IT Migrační dokumentace Licenční politika, certifikáty  |
|  |  | Řešení typických chyb a problémů Administrační nástroje Pravidelná údržba, profylaxe Popis Infrastruktury Datový model Kapacitní nároky – disky, HW Popis síťového řešení  |
| Zdrojové kódy  | Obecné požadavky na kód: * Snadná udržitelnost
* Vnitřní integrita
* Efektivita návrhu a zápisu
* Snadné další použití

Veškerý konfigurační kód musí být řádně okomentován tak, aby pro každý funkční modul bylo zřejmé: * Název modulu
* Účel modulu
* Původní autor
* Provedené změny (datum, autor, účel změny)

Veškeré názvy použité v konfiguračním kódu musí být uvedeny tak, aby byl odborným specialistům zřejmý účel pojmenovaného prvku v daném kontextu. Názvy musí odpovídat jmenné konvenci jednotné pro veškerý konfigurační kód v rámci dodávky. VZP preferuje standardizovanou konvenci CamelCase. Veškerý konfigurační kód musí být navržen v co nejjednodušší struktuře, která je zároveň čitelná a pochopitelná odborným specialistou. Odborným specialistou se myslí pracovník, který může být získán na běžném pracovním trhu a po absolvování běžně dostupného odborného výcviku může pracovat na dalších úpravách a rozvoji dodaného informačního systému.  |

**3. Infrastrukturní standardy**

## 3.1. HW

**On Premise** **Serverová infrastruktura**

Základem serverové infrastruktury, centralizované a provozované v rámci datových center (DC), jsou servery nebo serverovými systémy založené na architektuře procesoru x86. Serverová infrastruktura je postavena na neproprietálních základech (bez vazby na jediného konkrétního výrobce). Servery jsou certifikovány na operační systémy uvedené v kapitole 3. 3., musí být rozšířitelné, maximálně flexibilní a vysoce dostupné. Jednotlivé servery nebo serverové systémy jsou připojeny do sítě LAN a v případě komunikace s diskovými poli i do sítě SAN a vybaveny kvalitními nástroji pro správu. V případě používání virtualizace uvedené v kapitole 3. 3. je hardware management propojen s virtualizační vrstvou. Servery nebo serverové systémy jsou v provedení rackmount a v datových centrech jsou umístěny v rackových skříních velikosti 42U. Napájení rackových skříní se odvíjí od spotřeby zařízení, která jsou v něm umístěna.

**On Premise** **SAN infastruktura**

V jednotlivých datových centrech jsou primární disková enterprise a midrange pole, která jsou zapojena do SAN infrastruktury pomocí SAN přepínačů. Potřebná kapacita diskových polí je řešena rozšířením těchto polí nikoliv nákupem dalších polí. Do této SAN infrastruktury jsou z důvodu vysoké propustnosti a kvalitního zabezpečení (využití alternativních cest) zapojeny všechny významné servery, zálohovací knihovny a zmíněná disková pole. Tato SAN síť využívá u všech významných komponent minimálně 2 FC rozhraní pro zajištění vysoké dostupnosti.

Data kritických aplikací jsou umisťována na enterprise disková pole, data běžných aplikací a testovací prostředí pak na midrange disková pole.

## 3.2. Sítě

###  3.2.1. Celkové schéma sítě VZP ČR

Z hlediska vztahu k uživatelům a k okolnímu světu je možné počítačovou síť VZP ČR rozdělit do několika funkčních celků:

* **Perimetr**
* **Datová centra**
* **WAN síť**
* **LAN sítě ústředí, regionálních poboček a kliprů**

Schematicky je síť VZP ČR znázorněna na následujícím obrázku:



|  |  |  |
| --- | --- | --- |
|   |  |  |
| **CMS**  |   | Centrální místo služeb  |
| **GSM**  |   | Globální Systém pro Mobilní komunikaci  |
| **JTS**  |   | Jednotná telefonní síť  |
| **SUKL**  |   | Státní úřad pro kontrolu léčiv  |
| **RP**  |   | Regionální pobočka  |
| **KLIPR**  |   | Klientské pracoviště  |
| **DC1**  |   | Datové centrum 1 na adrese Orlická 4/2020, 130 00 Praha 3  |
| **DC2**  |   | Datové centrum 2 na adrese ČD Telematika, Pod Táborem 369/8a, 190 00  |
|   |   | Praha 9  |
| **LAN** **Orlická**  | Ústředí na adrese Orlická 4/2020, 130 00 Praha 3  |
| **LAN** **Crystal**  | budova Crystal na adrese, Vinohradská 2577/178, 130 00 Praha 3  |
| **LAN** **Kutvirtova**  | Call Centrum a klipr na adrese Kutvirtova 339/5, 150 00 Praha 5  |

###  3.2.2. LAN RP a KLIPRů

LAN ve VZP ČR je rozdělena do vrstev podle hierarchického modelu:

* **Access (přístupová) vrstva** – zajišťující konektivitu koncových uživatelů
* **Distribution (distribuční) vrstva** – zajišťující vysokou dostupnost
* **Edge (hraniční) vrstva** – slouží pro připojení LAN do WAN

#### SLUŽBY A TECHNOLOGIE LAN

* VLAN
* QoS

#### VLAN

VLANy jsou implementované v přístupové vrstvě. Uživatelé z různých oddělení, rozděleni do určených VLAN, mohou přistupovat do sítě určenými přístupovými přepínači, které jsou umístěny v různých podsítích. V hraniční, případně distribuční, vrstvě je nakonfigurované směrování těchto podsítí mezi sebou a také případné omezení provozu mezi VLANami pomoci ACL – Access Control List (přístupových listů).

#### QOS (QUALITY OF SERVICE)

QOS zajišťuje rovnoměrné vyvažování zátěže sítě s ohledem na druh přenášených dat, spravedlivě rozděluje konektivitu mezi jednotlivé aplikace dle nastavených priorit a zabraňuje přetížení sítě.

Ve VZP ČR jsou použity následující **QoS** třídy, které jsou řazeny dle priority – od nejvyšší priority po nejnižší prioritu.

* Třída – Network support
* Třída – Real time (VoIP RTP, VoIP Signalizace)
* Třída – 3B: Interaktivní provoz (terminálová třída) – (Aplikace Interaktivní)
* Třída – 3A: Web provoz (webová třída)
* Třída – 3D: Scavenger třída (DoS, P2P, ...) – Služby UDP (Bulk)
* Třída – Zbytková třída – ostatní provoz

###  3.2.3. Bezdrátová síť (WIFI)

Bezdrátová síť ve VZP ČR je provozována na standardních zařízeních a technologii firmy Cisco. Bezdrátová síť poskytuje několik variant připojení:

* **WLAN\_DATA** – síť určená pro standardní uživatele interní sítě VZP, je veřejně inzerovaná. Tato síť je určená pro běžného uživatele a jsou na ni implementovány bezpečnostní omezení.
* **WLAN\_ADMIN** – síť určená pouze pro administrátory sítě. Síť není veřejně inzerovaná (má vypnuto vysílání SSID).
* **WLAN\_PHONE** – síť určená pro připojení mobilních telefonů a pro volání po bezdrátové síti. Síť není veřejně inzerovaná (má vypnuto vysílání SSID). Přístup do sítě je ověřen pomocí MAC adresy zařízení.
* **WLAN\_GUEST** – síť určená pro připojení externích uživatelů s přístupem pouze do Internetu pomocí protokolu HTTP (S). Tato síť je veřejně inzerovaná.
* **WiredGuest** – jedná se o drátovou síť, která je řízená prostředky bezdrátové sítě a funguje obdobně jako síť WLAN\_GUEST s tím rozdílem, že klient se místo k bezdrátové síti připojuje do portu přepínače.

Tuto síť je možno využívat pouze v centrálních lokalitách – Orlická, Perštýn.

Tato síť určená pro připojení externích uživatelů s přístupem pouze na Internet.

####  3.2.4. WAN

VZP ČR provozuje privátní datovou síť WAN na přenosových prostředcích poskytovatele datového připojení pomocí technologie MPLS. Pro zajištění bezpečnosti přenášených dat je použito šifrování na síťové vrstvě mezi koncovými zařízeními pomocí protokolu IPSec. Pro navazování šifrované komunikace mezi směrovači v síti VZP ČR je použita technologie GET (Group Encrypted Transport) VPN. **Šířka pásma**

|  |  |  |
| --- | --- | --- |
| **Typ pobočky**  | **Počet uživatelů**  | **Šířka pásma**  |
| 1 | 1-5 | 0,5 Mbps |
| 2 | 6 -50 | 4 Mbps |
| 3 | 51 a více | 8 Mbps |

###  3.2.5. Datová centra On premise

VZP ČR provozuje dvě geograficky oddělená datová centra:

 ‒ DC1 na adrese Orlická 4/2020, 130 00 Praha 3

 ‒ DC2 na adrese ČD Telematika a.s., Pod Táborem 369/8a, 190 00 Praha 9

Obě datová centra jsou propojena dvěma nezávislými optickými trasami technologií DWDM. Jedna vlnová délka o kapacitě 10 Gbps je použita pro LAN provoz a druhá 10 Gbps pro propojení firewall clusteru. Pro propojení SAN přepínačů jsou multiplexovány dva kanály, každý o kapacitě 4 Gbps.



Každé z datových center VZP ČR je vytvořeno na technologii firmy Cisco Nexus dle architektury Spine and Leave a patří mezi tzv. aplikačně řízené infrastruktury (Application Centric Infrastructure ACI), které umožňují integrovat do řízení síťového provozu datového centra vlastní logiku jednotlivých aplikací z pohledu jejich požadavků na síťovou konektivitu, bezpečnost a L4-L7 služby (load balancing, firewalling atd.). Fyzické nebo virtuální aplikační servery sdílející stejnou bezpečnostní a síťovou politiku jsou konsolidovány do logických skupin a současně je definována jejich vzájemná komunikace (která aplikační komunikace je povolená, jaké vyžaduje QoS parametry a jaké vyžaduje L4-L7 služby).

Veškeré aplikační politiky jsou definovány na centrálním kontroleru (Application Policy Infrastructure Controller - APIC), který je s využitím otevřených aplikačních rozhraní automaticky distribuuje na jednotlivé komunikační prvky a systémy, které následně podle těchto aplikačních politik řídí síťový provoz.

#### Logická infrastruktura

Provoz datového centra je z pohledu toku dat směrem od uživatele k vlastním datům rozdělen do jednotlivých funkčních modulů neboli zón. Rozhodujícím hlediskem pro sledování toku dat je „kdo inicializuje komunikaci“.

Zóny představují zpravidla několik L3/L2 segmentů, která mají podobná bezpečnostní pravidla. Zóny jsou IP adresací příslušné k lokalitě DC. Výjimku tvoří zóna DC-DB, ta je L2 geograficky rozprostřena mezi lokalitami DC1 a DC2. **Rozdělení DC zón:**

 ‒ **Síť VZP ČR (VZP NET)**

Zóna označuje síť VZP, která není součástí DC – tj. infrastrukturní část LAN/WAN včetně části koncových uživatelů.

 ‒ **Demilitarizovaná zóna (DC-DMZ )**

Zóna je dostupná z obou stran jak pro VZP, tak pro DC. Slouží k zabezpečení a poskytování služeb. Typicky Management, DNS, MS AD DC nebo LDAP, ACS. Do této zóny patří vrstva správy a administrace a vrstva infrastrukturních serverů.

 ‒ **Prezentační vrstva** **(DC-VIP)**

Jedná se o vrstvu, v které jsou umístěné servery zajišťující komunikaci s uživateli. Patří sem i virtuální IP adresy, které reprezentují jednotlivé aplikace pro přístup jak z VZP NET, tak z ostatních aplikací DC.

 ‒ **Aplikační vrstva (DC-APP )**

Zde jsou umístěny aplikační servery zajišťující business logiku jednotlivých aplikací. ‒ **Databázová vrstva DC (DC-DB)**

Umístění DB serverů. L2 vrstva rozprostřená geograficky mezi lokalitami DC1 a DC2. V databázové vrstvě je možné vytvářet clustery se společnou IP adresou mezi jednotlivými lokalitami.

 ‒ **Servisní zóna (DC-SERVIS)**

Zóna slouží jako prostředník pro výměnu dat mezi ostatními zónami a mezi prostředími produkce a test.

Zóny DC-APP a DC-DB nejsou přímo dostupné z VZP NET a obráceně. Komunikace musí být zprostřed-kována přes některou ze zón DC-DMZ, DC-VIP, DC-SERVIS .

**Komunikační matice zobrazuje podporované komunikace mezi jednotlivými zónami.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|   |  | Komunikace do zóny →  |  |  |  |  |
| Komunikace zóny ↓  | ze  | VZP NET  | DC-DMZ  | DC-VIP  | DC-APP  | DC-DB  | DC-SERVIS  |
| VZP NET  |  | ANO  | ANO  | ANO  | **Ө**   | **Ө**   | ANO  |
| DC-DMZ  |  | ANO  | ANO  | ANO  | ANO  | ANO  | ANO  |
| DC-VIP  |  | **Ө**   | **Ө**   | **Ө**   | ANO  | **Ө**   | **Ө**   |
| DC-APP  |  | **Ө**   | ANO  | ANO  | **Ө**   | ANO  | ANO  |
| DC-DB  |  | **Ө**   | ANO  | **Ө**   | možné  | možné  | ANO  |
| DC-SERVIS  |  | ANO  | ANO  | **Ө**   | ANO  | ANO  | ANO  |

###  3.2.6. Perimetr

Perimetr je zabezpečená oblast podnikové sítě, která leží mezi internetem a vnitřní sítí VZP ČR.

Perimetr je rozdělen pomocí bezpečnostních bran (firewallů) do několika oddělených bezpečnostních zón:

* vnější perimetr – bezpečnostní oddělení externích sítí (Internetu) od sítě VZP
* vnitřní perimetr – bezpečnostní oddělení veřejně vystavených služeb VZP od vnitřní

(uživatelské) sítě VZP

Součástí řešení je i VPN přístup do VZP ČR. VPN slouží pro vzdálený přístup zaměstnanců a externích kontraktorů do sítě VZP ČR z Internetu.

###  3.2.7. Síťové služby

Síť VZP ČR poskytuje pro koncová zařízení, aplikace a uživatele následující služby:

 ‒ Časová synchronizace (NTP)

 ‒ Kvalita služby (QoS)

 ‒ DNS, DHCP, IPAM (DDI)

 ‒ Loadbalancing

###  3.2.8. Sjednocená komunikace

Sjednocená komunikace je ve VZP ČR tvořena následujícími součástmi:

‒ **Hlasová komunikace** o IP Telefonie o Integrované nadstavbové funkcionality o Spolupracující systémy

* Call Centrum Atlantis
* Cisco Paging

‒ **Elektronická komunikace** o Instant messaging - Cisco Jabber o Webová konference – Cisco WebEx

## 3.3. OS

V době instalace musí mít všechny implementované verze OS zajištěnu podporu ještě minimálně dalších 5 let.

###  3.3.1. OS pro aplikace třídy A

* Red Hat Enterpise Linux, Oracle Linux, CentOS (verze 7 a vyšší)
* MS Windows Server 2012R2 EN, 2016 EN

###  3.3.2. OS pro aplikace třídy B

Red Hat Enterprise Linux, Oracle Linux, CentOS (verze 7 a vyšší)

MS Windows Server 2012R2 EN, 2016 EN

###  3.3.3. Prostředí pro virtualizaci

Hostitelský systém je hypervizor nebo operační systém s hypervizorem , který umožní provoz Virtuálních serverů. Podporované platformy jsou a ve VZP mohou být nasazeny technologie, VMWare vSphere 5.5 Enterprise a vyšší a MS Hyper-V 2012R2 a vyšší.

Řízení Virtuálních serverů - správa VMs na VMWare nástrojem VMWare vCenter Server 5.5 Standard a vyšší. Správa VMs na Hyper-V je realizována nástrojem SCVMM 2012R2 a vyšší.

Pro zajištění vysoké dostupnosti aplikací třídy A pro a realizaci DRP plánu slouží technologie VMware DRS a HA cluster, případně VMware SRM, VMware vSAN nebo MS Hyper-V Clustering, MS Storage Spaces Direct v aktuálních verzích.

U aplikací třídy B lze použít i další virtualizační technologií:

 KVM (Kernel-based Virtual Machine)

###  3.3.4. Požadavky na linuxové účty

Uvedené požadavky jsou se zdůrazněním požadavků na aplikace ve vztahu k administraci.

* Na linuxových systémech se rozlišují 2 typy účtů: uživatelské a servisní účty.
* Uživatelské účty jsou centralizované, autentizace protokolem Kerberos, autorizace protokolem LDAP. Autentifikace i autorizace je nezávislá na aplikačním IDM. Zřizovány jsou pouze za účelem správy systému, subsystémů a aplikací. Je zakázáno přidělovat uživatelské účty kvůli aplikačním přístupům (např. pro přenosy dat do/z aplikace). Na uživatelské účty se vzdáleně přistupuje protokolem ssh, autentizace heslem (možno GSSAPI).
* Servisní účty, to jsou účty dedikované pro správu, instalaci, provoz systému, subsystémů (např. Oracle db, aplikační servery, aj.) a aplikací, jsou lokální. Servisní aplikační účty (a skupiny) jsou alfabetické malými písmeny, začínají znaky ‚vzp‘, dále identifikace aplikace. Primární skupinou servisního aplikačního účtu je skupina stejného jména. S omezením na 16 znaků. UID a GID pro subsystémy a aplikace jsou přidělovány jednotně centrální autoritou VZP. Na servisní účty za účelem administrace se přistupuje pomocí sudo z běžného uživatelského účtu na základě přidělené administrátorské role (dedikovaný administrátorský LDAP). Přístup na servisní účty není povolen s autentifikací heslem.
* Instalace dané aplikace včetně tvorby unixové adresářové struktury (vlastnictví, skupiny uživatelů, práva) se provádí na základě aplikační dokumentace pomocí dodané instalační úlohy. Aplikační dokumentace musí obsahovat seznam veškerých aplikačních trustů vytvářených na úrovni systému (ssh public key trusty pro vzájemnou komunikaci, aj.). Aplikace obsahuje úlohu, která kontroluje správnost nasazení, tedy mj. i nastavení vlastnictví, skupiny uživatelů, práva v adresářových stromech aplikace. Zjištěné chyby jsou protokolovány, a pokud je to možné, automaticky opravovány.
* Veškeré aplikační struktury jsou uchovávány v dedikovaných aplikačních adresářových stromech. Pokud aplikace využívá obecné subsystémy (např. java, http server, openssl, …), musí být rovněž veškerá konfigurace a data těchto subsystémů v adresářových stromech aplikace a nezávislá na případném použití komponenty jinou souběžnou aplikací (dedikovaný port pro http server, …). Pokud nelze zajistit nezávislost použití dané komponenty, musí aplikace použít vlastní instalaci komponenty ve svém aplikačním stromě.

## 3.4. Middleware

###  3.4.1. Integrační platforma

* je založená na koncepci ESB (Enterprise Service Bus) jako podnikové sběrnice služeb  pro realizaci integrace aplikací a služeb
* využívá centrální business rule repozitory a Business rule engine
* využívá principy servisně orientované architektury (SOA)
* využívá MOM architekturu (Message Oriented Middleware) jako podmnožinu ESB kde prostřednictvím Message brokera zajišťuje spolehlivé doručení zprávy nesoucí informaci (Message) mezi jednotlivými systémy (prostřednictvím front).
* využívá model řízení událostmi

**Integrační platforma poskytuje tyto typy služeb:**

* centrální řízení komunikaci mezi systémy realizované prostřednictvím ESB služeb,
* kompozice vlastních služeb a jejich publikace konzumentům
* zprostředkování a publikace sdílených služeb konzumentům,
* orchestraci služeb vnitřních i vnějších s ostatními integračními technologiemi (BPEL)
* směrování a předávání dat mezi jednotlivými službami
* transformaci formátů dat,
* konverze protokolů mezi jednotlivými službami,
* centrální business rule repozitory
* centrální repozitory služeb

###  3.4.2. Aplikační servery

Výčet typů AS využívaných v IS VZP:

|  |  |
| --- | --- |
| **Druh AS**  | **Použití**  |
| Oracle Fusion Middleware WebLogic Server v nejnovější podporované verzi  | Aplikace deployované v J2EE, vhodné pro aplikace třídy A  |
| JBoss aplikační server v nejnovější podporované verzi  | Pro J2EE aplikace třídy B nebo v odůvodněných případech, kde není vhodné použití Oracle Weblogic J2EE.  |

###  3.4.3. Webové servery

Výčet typů WS využívaných v IS VZP:

* Oracle Web Tier v nejnovější podporované verzi
* Apache v nejnovější podporované verzi
* IIS

## 3.5. Virtualizovaná infrastruktura pro hostování aplikací

Aplikační služby jsou hostovány na virtuálních prostředí / serverech následujících parametrů:

|  |  |
| --- | --- |
| **Název služby**  | **Popis**  |
| Server s OS  |  OS Windows nebo Linux (viz kap. 3.3 OS)  |
| Aplikační server  | OS Windows nebo Linux aplik. serveru Oracle Weblogic Suite  |
| Databázový server Oracle  | OS Linux, Oracle dB EE + RAC + partitioning  |
| Databázový server MS SQL  | OS MS Windows, MS SQL Server v edici Enterprise  |

## 3.6. Deployment aplikací NIS do prostředí v DC

Pro zabezpečení provozu aplikací v prostředí datových center je používán standardizovaný deployment aplikací :

* Produkční instance aplikací a jejich odpovídajících dat je hostována v primárním datovém centru na zařízeních s vysokou dostupností a redundancí na virtualizované infrastruktuře.
* Záložní instance aplikací je hostována ve virtualizované infrastruktuře v záložním datovém centru s dedikovanou kapacitou úložiště o velkosti produkčních dat pro fail over primárního DC.
* Virtualizovaná infrastruktura serverů záložního centra je dimenzována jako výkonový ekvivalent zařízení v primárním datovém centru. Požadavek na dostupnost je nižší, tomu odpovídá nižší redundance prvků.
* Virtualizovaná infrastruktura záložního centra je sdílena s testovacími prostředími.
* Produkční data z primárního DC jsou asynchronně replikována do záložního DC.
* Pro účely testování je v záložním DC dedikována obecně kapacita virtualizované úložné kapacity až v rozsahu 1,2 velikosti produkčních dat sdílená pro všechny instance testovacích prostředí. Tato kapacita je alokována individuálně při návrhu systému.

Datové centrum

1

-

záložní

Testovací

,

vývojové prostředí a záložní produkční prostředí

Datové centrum

2

-

primární

Produkční prostředí

Storage A

Produkční

**kapacita A**

**/**

redundantní prvky řešení pro

vysokou dostupnost

Apl

1

FO

TP

1

Legenda

:

APL

=

hostovaná aplikace

AS

-

aplikační server

DS

-

databázový server

FO

–

Fail over prostředí

TP

-

klon testovacího prostředí

kapacita P

=

výkonová kapacita aplikačních nebo DB serverů

kapacita A

,

B

=

objemová kapacita datových úložišť

**B**

**1**

**=**

**1**

**A**

Kapacita pro fail over

řešení velikosti produkční

kapacity

**B**

**2**

**=**

**1**

**,**

**2**

**A**

Kapacita pro

testovací prostředí

Snížené nároky na dostupnost

Storage B

TP n

…

.

Virtualizované AS

,

ka

~~pa~~

cita

1

,

2

P

Virtualizované DS

,

kapacita

1

P

**R**

**e**

**p**

**l**

**i**

**k**

**a**

**c**

**e**

**d**

**a**

**t**

**p**

**r**

**o**

**F**

**O**

**F**

**a**

**i**

**l**

**o**

**v**

**e**

**r**

**p**

**ř**

**e**

**p**

**n**

**u**

**t**

**í**

**P**

**ř**

**i**

**d**

**ě**

**l**

**e**

**n**

**í**

**z**

**d**

**r**

**o**

**j**

**ů**

Apl

1

Prod

Apl N

Prod

Virtualizované AS

,

kapacita P

Virtualizované DS

,

kapacita P

**P**

**ř**

**i**

**d**

**ě**

**l**

**e**

**n**

**í**

**z**

**d**

**r**

**o**

**j**

**ů**

## 3.7. Datové a databázové služby

#### 3.5.1. Databázové technologie

|  |  |
| --- | --- |
| **Standard**  | **Popis**  |
| Oracle DB EE v nejnovější podporované verzi, včetně databázových options  | Pro aplikace třídy A nebo B.  |
| MS SQL EN v nejnovější podporované verzi,X64bit  | Podpůrné služby a pro aplikace v třídě B. V odůvodněných případech je možné použít i pro aplikace třídy A.  |

#### 3.5.2. Datové a databázové standardy

|  |  |
| --- | --- |
| **Oblast standardizace**  | **Popis**  |
| Minimum redundancí  | Data jsou uložena v jediné databázi. Redundantní databáze v rámci lokality nejsou pro core business aplikace povoleny. Replikace se provádí pouze z důvodu realizace DR plánu..  |
| Jediný zdroj informací  | Data jsou uložena v místě jejich vzniku, do ostatních systémů jsou poskytována prostřednictvím integrační platformy. Platí pravidlo minima duplicit.  |
| Datová konzistence  | Datová konzistence je zachovávána již v rámci databáze, tedy nikoliv pouze aplikačně.  |
| Modelování DB pomocí ER diagramu  | Jsou zachovány normálové formy. Pouze v případech, kdy je to nutné jsou možné výjimky – v dokumentaci však je explicitně uvedeno.  |
| Návrh datového modelu  | Návrh datového modelu DB musí být akceptován datovým architektem VZP ČR. Persistentní objekty vývojář definuje bez určení: * Názvu tablespace
* fyzických atributů segmentu (pctused, pctfree, storage params,...)

Databázové objekty jsou považovány za privátní součást aplikace, tzn. aplikace může přistupovat k databázovým objektům jiné aplikace pouze prostřednictvím dedikovaných služeb.  |
| Jmenné konvence databázových objektů  | Všechna jména základních databázových objektů (tabulky, pohledy, balíky funkcí a procedur, fronty, sekvence, indexy, triggery apod.) začínají dvouznakovým prefixem dodavatele  |
| Kódování  | Preferované UTF16, UTF8, Definici collation – preferována Czech CI AS (case insensitive a accent sensitive) Na výjimku: ISO 8859-2, Windows 1250  |
| Podpora anonymizace / pseudonymizace osobních údajů  | Datová vrstva musí podporovat možnost anonymizace a pseudonymizace osobních údajů bez nežádoucí vlivu na chování datového engine a aplikace. Využívá se pro účely příslušné legislativy a vytváření datového derivátu pro testování z produkčních dat. Součástí dodávek je nástroj pro vytváření anonymizovaných derivátů produkčních dat (scrambling tool). Toto musí být zohledněno i v dokumentaci.  |
| Podpora řezů dat  | Datový model musí být navržen tak, aby pro účely testování bylo možno oddělit testovací derivát – vzorek dat z produkčních dat. Součástí dodávek je nástroj pro vytváření takových derivátů. Toto musí být zohledněno i v dokumentaci.  |
| Zakázané vazby  | Data v relačních databázích nesmí být provazována technologicky přes významové klíče, povolena je relační vazba pouze přes nezávislé technologické klíče záznamů. Nejsou dovoleny přímé datové vazby mezi datovými doménami.  |

## 3.6. Koncová zařízení

* Koncová pracovní zařízení počítače a notebooky o Instalován OS Windows 7/10 enterprise x64/x32
	+ Nastavení OS systému a uživatelského prostředí řízeno centrálně doménovou politikou.
	+ Uživatel nemá na koncové zařízení administrátorské práva o Vzdálený přístup je zajištěn Remote Desktop, Support Assistant o Aktualizace OS v 6 měsíčním cyklu

* Programové vybavení koncových pracovních zařízení o MS Office 2010/16 Profesionál plus o Google Chrome, nastavení řízené centrální doménovou politikou o IE aktuální verze 11, nastavení řízené centrální doménovou politikou o 7ZIP
	+ Cisco AnyConnect Secure Mobility Client (Notebooky)
	+ Adobe Reader 11/DC

* Centrální distribuce programového vybavení na pracovní stanice o Distribuce SW je použitím SCCM

* Zabezpečení koncových pracovních zařízení o Endpoint Protection , Antivirová ochrana Kaspersky Endpoint Securit (centrálně řízený)
	+ - AntiMalware, IDS/IPS,
		- Firewall,
		- Application control,
		- Device control,
		- Antispam

* Jednotná adresářová struktura  Root: APPL

Archiv

Data

Nezalohovano

Program Files

Temp

TMP

Users

Windows

* + Pro Root, Program Files, Windows má běžný uživatel práva pouze pro čtení

* Ostatní programové vybavení o JAVA 1.6.045 ,1.7.51 , 1.8. 111
	+ NET Framework ver. 4.0 a vyšší

* Tisková koncová zařízení o Tisková a multifunkční zařízení připojená přes tiskový server, výjimečně lokální připojení
	+ Follow me printing se zabezpečeným tiskem. o Ověřování pomocí bezkontaktních karet o (embeded čtečka v MFDnebo externí terminál, možnost ověření PINem). o Scan to me (možnost naskenovat z jakékoli MFD a obdržet sken v personální složce nebo emailem).

* Ostatní koncová zřízení o Mobilní telefony s OS : Android 5.0 a vyšší, Windows 10 mobile

## 3.7. Elektronická pošta

* Elektronická pošta ve VZP ČR je realizována prostřednictvím Microsoft Exchange 2010. Příjem elektronické pošty z Internetu zajišťují dedikované SMTP brány v perimetru, před předáním zpráv do interního poštovního systému je provedena jejich antivirová a antispamová kontrola. Odesílání pošty mimo lokální poštovní doménu probíhá pomocí SMTP protokolu s využitím poštovních bran.
* Klientský přístup k poštovnímu systému je zajištěn pomocí MS Outlook verze 2010 nebo 2016, případně prostřednictvím internetového prohlížeče (Outlook Web App). Poštovní systém podporuje kromě SMTP i protokoly POP3 a IMAP.

 Poštovní systém je využíván pro strategické řízení firmy, a proto je implementován jako vysoce dostupný.

## 3.8. Active Directory

VZP ČR využívá pro ověřování uživatelů a pracovních stanic Microsoft Active Directory (dále AD). Služby AD jsou realizovány na serverech s MS Windows Server 2012 R2. V AD má každý uživatel i každá pracovní stanice svůj účet. Účty uživatelů jsou spravovány prostřednictvím Identity Managementu na základě údajů uložených v personálním systému. AD zajišťuje pomocí skupinových politik i nastavení pracovních stanic v souladu s platnými bezpečnostními standardy.

## 3.9. PKI

VZP ČR využívá systém interních certifikačních autorit (PKI) založený na Microsoft Windows Server 2008 R2. Vystavované certifikáty slouží pro identifikaci pracovních stanic a serverů v interní síti VZP ČR a dále pro podpis a šifrování elektronické pošty a pro vzdálený VPN přístup uživatelů do VZP ČR.

**4. Bezpečnostní standardy**

## 4.1. Dodržování legislativních požadavků

V rámci dodávky je požadováno striktní dodržování zejména:

* Zákon o ochraně osobních údajů (zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, v platném znění.)
* Autorský zákon (zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů, v platném znění.)
* Zákon o Kybernetické bezpečnosti (zákon č. 181/2014 Sb. v platném znění)
* NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679

## 4.2. Dodržování obecných standardů a doporučení

V rámci dodávky/vývoje je doporučeno dodržování obecně platných standardů, zejména:

* RFC
* CIS (Center for Internet Security Benchmark)
* OWASP
* ISO/IEC 2700x *(ISMS)*
* ISO/IEC 12207 *(Systems and software engineering – Software life cycle processes)*
* ISO/IEC 15504 *(Software Process Improvement and Capability Determination (SPICE))* Výjimky nebo odchylky od uvedených standardů musejí být předem schváleny VZP.

## 4.3. Minimalizování běžících služeb

Na serverech jsou nainstalovány a běží pouze takové služby, které jsou nezbytné pro korektní běh aplikací nebo správy systému. Ostatní služby musí zůstat vypnuté.

## 4.4. Nevyhovující služby nebo protokoly

Služby nebo protokoly, které nevyhovují bezpečnostním požadavkům pro přenos či zpracování definované kategorie citlivosti informace nesmí být pro přenos nebo zpracování informace použity.

Nevyhovuje zejména:

* použití nešifrovaných protokolů pro vzdálenou administraci (TELNET, http, atd …)
* použití nešifrovaných protokolů pro přenos dat (FTP, http, atd …)
* použití slabých a již nevyhovujících metod šifrování (SSL2, SSL3, SHA1, atd…) (viz. minimální požadavky na šifrování)
* použití služeb se známou zranitelností, která není výrobcem opravena nebo je neopravitelná  použití služeb bez podpory výrobce (Out Of lIfe)

## 4.5. Minimální požadavky na šifrovací algoritmy

Obecně kryptografické algoritmy musí vždy splňovat požadavky ZoKB (181/2014) a vyhlášky 316/2014.

Použití konkrétního algoritmu podléhá schválení VZP. Jsou preferovány následující algoritmy:

Advanced Encryption Standard (AES) s využitím délky klíčů 256 bitů, SHA-2, SHA-256

## 4.6. Mechanismus obrany proti hádání přístupu do systému

Ve všech systémech nebo aplikacích musí být implementována kontrola proti pokusům o uhádnutí uživatelských jmen a hesel (např. prostřednictvím omezeného počtu pokusů o přihlášení a definované doby omezení přístupu do systému či aplikace). V případě několika neoprávněných přístupů musí dojít k automatickému uzamčení postiženého účtu. (Nevztahuje se na systémové účty, které to neumožňují. Např. administrátor u win, nebo je tato funkce z provozních důvodů nežádoucí. U těchto účtů musí být nastaveno velmi silné heslo.) Opětovné odemknutí je v kompetenci Administrátora systému nebo aplikace. Navržený mechanismus musí být navržen tak, aby nedošlo k hromadnému zamykání a tím odepření služby.

## 4.7. Důvěrnost

###  4.7.1. Klasifikační schéma informačních/datových aktiv

Pro účely klasifikace informací VZP ČR je stanoveno následující klasifikační schéma informací:

1. **chráněné** informace **–** informace, jejichž ochrana vyplývá ze zákona, nebo informace vyžadující zvýšenou úroveň ochrany na základě obchodních nebo vnitřních požadavků z hlediska dostupnosti, důvěrnosti nebo integrity,
2. **interní** informace **–** informace související s běžným provozem VZP ČR a jednotlivých organizačních celků, které nejsou určeny ke zveřejnění a nesmějí být volně přístupné externím subjektům,
3. **veřejné** informace **–** informace, které nevyžadují žádný zvláštní stupeň ochrany ve vztahu k zachování důvěrnosti, dostupnosti a integrity. Tyto informace mohou být volně zveřejněny i mimo VZP ČR.

###  4.7.2. Bezpečnost umístění informačních/datových aktiv/souborů

* Úložiště datových aktiv musí umožnit řízení přístupových oprávnění pro jednotlivé uživatele a na jednotlivá aktiva.
* Řízení přístupových oprávnění musí být integrovatelné/napojitelné s/na Active Directory VZP.
* Úložiště musí umožnit auditing operací s jednotlivými aktivy – logování přístupů a operací (File Auditing)
* Úložiště musí logovat neúspěšné pokusy o přístup.
* Úložiště musí podporovat napojení logů na SIEM a Centrální úložiště logů (*viz. Nepopíratelnost - Požadavky na auditing*)
* Úložiště musí umožnit napojení na systémy ochrany proti malware. Nebo jinak zabránit uložení a šíření škodlivého kódu a zajistit možnost pravidelné antivirové kontroly.
* U diskových polí je doporučené/preferované napojení pomocí ICAP nebo RPC.

###  4.7.3. Bezpečnost přenosu dat

* Pokud jsou chráněné informace přenášeny po síti, musí být během přenosu šifrována. Nebo musí být zajištěno šifrování komunikační linky bez ohledu na přenášená data. Toto neplatí pro komunikace v rámci datového sálu VZP ČR.
* Pokud jsou chráněné informace uloženy na nosičích, ať již pro potřeby přenášení informací či z důvodu zálohy, musí být zašifrována.
* V rámci dokumentace a testování nesmí být použita osobní nebo citlivá data. Taková data musí být anonymizována.
* Anonymizací se rozumí taková úprava, po které nelze údaje vztáhnout k určenému nebo určitelnému subjektu údajů.
* Jakýkoliv privátní klíč uživatele musí být chráněn heslem.
* Privátní klíče musí být spolehlivě zálohovány pro případ jejich ztráty nebo poškození.
* Musí být definovány postupy pro obnovení klíče a postupy instalace nového klíče v případě nedůvěry ve starý aktuální klíč.
* Přenos dat pomocí nosičů (uložení data na nosič) musí být logován a log archivován. Logy musí být předávány do SIEM a Centrálního úložiště logů (*viz. Nepopíratelnost - Požadavky na auditing*).

###  4.7.4. Popis umístění dat a jejich životní cyklus

####  Data at rest – Data v klidu

* K datům v úložišti musí být řízen přístup a musí být zajištěno, že se k nim dostane pouze oprávněná osoba a bude jí umožněno s nimi nakládat jen způsobem, který odpovídá její úrovni prověření.
* Pokud hrozí, že úložiště může být fyzicky ukradeno, musí být chráněné informace na úložišti šifrovány.
* Pro případ zničení dat musí být data zálohována a archivována. Média se zálohou musí být umístěna v geograficky vzdálené lokalitě, nebo tak, aby nehrozilo současné zničení medií a zdrojových dat.
* Zálohovaná data se musí podepisovat nebo vytvářet kontrolní součty.
* Musí být nastaven proces pro bezpečnou likvidaci již nepotřebných informací, tak aby je nešlo snadno obnovit.

Operace (vytvoření, modifikace, smazání a v případě citlivých dat i čtení) s uloženými daty musí být logovány a log archivován. Logy musí být předávány do SIEM a Centrálního úložiště logů (*viz. Nepopíratelnost - Požadavky na auditing*).

####  Data in motion – Data v pohybu

* Během přenosu z/do úložiště musí být data chráněna proti odposlechu (Viz. Bezpečnost přenosu dat.)
* Je doporučeno jednotlivé zprávy číslovat, aby bylo zřejmé, že dorazily ve správném pořadí nebo že se někdo nepokusil o tzv. replay attack.
* Jako ochranu před nežádoucí modifikací je možné data podepsat a tím podvrženou nebo pozměněnou zprávu snadno odhalit.
* Přenos dat z/do úložiště musí být logován a log archivován. Logy musí být předávány do SIEM a Centrálního úložiště logů (viz. Nepopíratelnost - Požadavky na auditing).

####  Data in use – Data v použití

* Přístup k datům musí být řízen na základě přidělených oprávnění.
* Aktivity uživatele v systému musí být auditovány/logovány. Logy musí být předávány do SIEM a Centrálního úložiště logů (viz. Nepopíratelnost - Požadavky na auditing).
* V případě přístupu k osobním údajům musí logy odpovídat požadavkům zákona č. 101/2000 a „NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679“

## 4.8. Kompatibilita s DR (Disaster Recovery)

 Aplikace/dodávka musí zahrnovat stanovení procesů, postupů a opatření pro zajištění obnovy provozu a testování DR plánů.

## 4.9. Integrita dat

* Aplikace musí zajistit kompletnost a platnost dat při zaručeném zpracování pouze autorizovanými systémy a uživateli.
* Nesmí umožnit neautorizovaný zásah do evidovaných informací / dat.

## 4.10. Nepopiratelnost

###  4.10.1. Obecné požadavky na auditing/logování

Veškeré činnosti v systému musí být logovány a to včetně neúspěšných pokusů. Jde zejména o následující činnosti:

1. přihlášení a odhlášení uživatelů a administrátorů,
2. činnosti provedené administrátory,
3. činnosti vedoucí ke změně přístupových oprávnění,
4. neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
5. zahájení a ukončení činností technických aktiv,
6. automatická varovná nebo chybová hlášení technických aktiv,
7. přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a
8. použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.
9. Operace provádějící operace transakce s daty a to zejména citlivými, hromadnými a to jak na základě interakce uživatele tak na základě systémových událostí (např. nastalý čas)

V případě přístupu k osobním údajům musí logy odpovídat požadavkům zákona č. 101/2000 a „NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679“

### 4.10.2. Aplikační auditní log[[1]](#footnote-1)

* Každá komponenta, která se podílí na zpracování transakcí včetně volání služeb ESB bude logovat do lokálního transakčního logu. Do logu se zaznamenávají minimálně události volání a ukončení služby.
* Každý záznam je označen časovým razítkem vytvoření / modifikace záznamu.
* Toto platí bezpodmínečně pro služby manipulující s osobními daty, jak pasivními, tak služby měnící obsah ukládané informace.
* Výčet zaznamenávaných událostí odpovídající business logice je povinnou součástí návrhu a dokumentace systému.
* Lokální záznamy budou přenášeny k dalšímu zpracování do centrálního zpracování dle těchto razítek.

Informační obsah zaznamenávané události:

|  |  |  |
| --- | --- | --- |
| **Název**  | **Typ**  | **Popis**  |
| KOMP  | VARCHAR2  | Jednoznačný identifikátor komponenty, ze které je logováno  |
| ID\_SL  | VARCHAR2  | Identifikátor služby  |
| ID\_INST  | VARCHAR2  | Jednoznačný identifikátor instance dané transakce/služby přidělovaný zapisující službou  |
| POZADUJICI  | VARCHAR2  | Jednoznačný identifikátor komponenty/služby požadující službu  |
| ID\_SLP[[2]](#footnote-2)  | VARCHAR2  | ID služby předchozí  |
| ID\_INSTP2  | VARCHAR2  | Identifikátor běhu transakce/služby bezprostředně iniciující danou transakci/službu = (LTL.ID, LTL.KOMPONENTA)  |
| KOMPM2  | VARCHAR2  | ID mateřské komponenty  |
| ID\_SLM  | VARCHAR2  | IS služby mateřské  |
| ID\_BUS  | VARCHAR2  | Identifikátor primární business transakce – události předávaný přes všechna volání podřízených služeb  |
| ID\_PARTNER[[3]](#footnote-3)  | VARCHAR2  | Technologický identifikátor partnera, kterého se volání služby týká, předávaný přes všechna volání podřízených služeb.  |
| ID\_UZIV  | VARCHAR2  | Identifikace uživatele, který spustil primární službu. Předávaný přes všechna volání podřízených služeb.  |
| ID\_STAVSL  | VARCHAR2  | Stav dané instance transakce/služby = (Přijetí požadavku na službu, ukončení požadavku) Zaznamenává se minimálně volání a ukončení služby.  |
| VYST\_KOD  | VARCHAR2  | Výstupní stav dané instance transakce/služby = (ZPRACOVANO OK, NOK …..)  |
| CAS\_ZAP  | DATETIME  | Datum a čas zápisu záznamu  |

###  4.10.3. Nástroje auditu/logování

* Logy musí být k dispozici v parsovatelném formátu (např. csv), nebo k nim musí existovat nástroj na práci s daným typem logu. Všechny logy by měly být ukládány v produkčním systému a být zpětně k dispozici minimálně po dobu 30 dní.
* Logy musí být online pomocí protokolu SYSLOG předávány do centrálního úložiště logů.
* V případě, že není možné zajistit online předávání logů musí být zajištěno dávkové předávání a to buď pomocí protokolu FTP nebo CIFS(Samba).
* Logy musí být předávány do SIEM, a to buď nativně nebo universálním formátem „Common Event Format (CEF)“ případně dle RFC 3164 a 5424.
* Veškeré události spojené se změnou bezpečnostních parametrů jsou logované a auditovatelné.

###  4.10.4. Požadavky na ověření a sledování identity uživatele IS

**Identifikace interního uživatele**

* Identita interního uživatele je uchovávána v AD.
* Autentikace/ověření uživatele musí probíhat proti Active Directory.
* Autorizace interního uživatelek funkcionalitám systémů je řízena IDM (Identity Management Systém)

**Identifikace externího uživatele**

(např. klient přistupující na portál VZP):

* Identita uživatele je uchovávána v EIM (Externí Identity Management).
* Identita uživatele v systémech je řízena EIM
* Autentikace/ověření uživatele musí probíhat proti musí být napojeno na EIM pomocí SSO.

**Hesla**

* nesmí být uchovávána v čitelné podobě v dávkových souborech, automatických přihlašovacích skriptech, makrech, zkratkových klávesách, v nechráněných systémech a všude jinde, kde by mohlo dojít k jejich odhalení.

###  4.10.5. Přístupová práva uživatelů IS

* Identita konkrétního uživatele je ověřena z front-endu aplikace a propagována až ke koncovým službám přes všechny technologické vrstvy IS. K tomu je využíváno předávání autorizačního tokenu mezi službami (OAuth, SAML)
* Aplikace /dodávka musí umožnit napojení na IDM VZP, ve kterém jsou role a profily uživatele definovány.
* Musí být zajištěno řízení přístupů k jednotlivým aktivům na základě rolí nebo profilů v nástroji pro řízení identity a autorizace přiřazené konkrétnímu identifikovanému uživateli

## 4.11. Penetrační testy

* Předávaná aplikace/dodávka musí být ve spolupráci s dodavatelem podrobena internímu penetračnímu testu/testu zranitelnosti aplikace.
* V případě, že aplikace bude dostupná z internetu musí být proveden nezávislý penetrační test jako součást dodávky. Nebo jinak deklarovat, že dodávka je odolná známým zranitelnostem.

**5. Provozní standardy**

## 5.1. Monitoring

### 5.1.1. Rozsah monitoringu

Služba dohledu provozu informačního systému je centralizovaná a je zajišťována dohledovým centrem s dvousměnným provozem v pracovních dnech od 6:00 do 22:00 hod. (v režimu 5x16). V těchto časových úsecích jsou drženy pohotovosti řešitelských skupin pro síťovou infrastrukturu, operační systémy Unix, operační systémy Windows, Oracle infrastrukturu (databáze a middleware), provoz aplikací, Exchange, a pro dohledové nástroje.

Z hlediska teorie spolehlivosti IT systémů a služeb jsou sledovány a vyhodnocovány:

 chybovost, resp. dostupnost systémů a služeb (Availability) a jejich vytížení (Utilization),  výkonnost služeb (Performance).

Z technicko-provozního hlediska je monitoring provozován ve dvou hlavních úrovních – infrastrukturní a aplikační.

* Infrastrukturní monitoring pokrývá všechny prvky produkční IT infrastruktury ZIS od síťových prvků přes servery, databáze až po middleware. Je vyhodnocována dostupnost, resp. chybovost, jakož i vytíženost sledovaných prvků.
* Aplikační monitoring je zaměřen na sledování klíčových služeb produkčních aplikací. Probíhá aktivně pravidelným spouštěním aplikačních úloh, simulujícím uživatelské akce. Zároveň jsou pasivně vyhodnocovány vybrané úlohy reálných uživatelů. Je vyhodnocována dostupnost úloh a služeb, a současně jsou zaznamenávány a vyhodnocovány odezvy takto měřených transakcí, tedy výkonost aplikací. Výstupy pasivního monitoringu jsou využitelné pro sledování vytíženosti sledovaných oblastí.

### 5.1.2. Používané dohledové nástroje pro On premise řešení

Centrální systém dohledu provozu informačního systému je vybudován na platformě **HP Operations Manager** (HP OM). Do dohledového centra HP OM (centrální konzole) jsou soustřeďovány všechny důležité zprávy z ostatních monitorovacích nástrojů.

* **HP OM** – agent na úrovni OS, centrální konzole
* **HP OM Performance Manager** **(PM)** – sledování vytíženosti systémů
* **Oracle Enterprise Manager Cloud Control** **(OEM)** – agent, integrace vybraných událostí do HP OM
* **Microsoft System Center 2012 Operations Manager (SCOM)** – agent na úrovni OS, integrace vybraných událostí do HP OM
* **Nagios** – bezagentní, s integrací vybraných zpráv do HP OM
* **HP Business Service Management** **(HP BSM)** – integrace do HP OM o **Business Process Monitor (BPM)** – aktivní aplikační monitoring o **Real User Monitoru (RUM)** – pasivní aplikační monitoring
* **HP Network Node Manager i** **(HP NNMi)** – aktivní SNMP poll, pasivní SNMP trap, je integrován s HP OM
* **HP SiteScope** – bezagentní, integrace do HP OM a HP BSM

Není-li možné nasadit monitoring pomocí zavedených nástrojů, poskytne dodavatel v rámci dodávky aplikace monitorovací nástroj (například skript), jehož výstup lze integrovat do HP OM.

### 5.1.3. Požadavky na procesy z hlediska monitoringu

* Aplikační monitoring musí být součástí nasazovaného systému.
* Kritické a závažné chybové stavy procesů/aplikací, které brání jejich provozu, dále chyby automatizovaných a dávkových zpracování musejí být zapisovány do aplikačního logu. Formát logu je popsán dále v odstavci pro rozhraní monitoringu.
* Obchodně kritické procesy by měly mít implementovánu striktně čtecí roli pro technologického uživatele monitoringu, pokud tomu nebrání samotná povaha procesu (např. plně aktivní operace). Tato role musí umožnit i odstraňování případných sestav vytvářených uživatelem.
* Součástí akceptačních testů musí být ověření funkčnosti monitoringu.

### 5.1.4. Požadavky na návrh monitoringu

Každá nově dodávaná aplikace nebo komponenta infrastruktury musí být monitorována, a to před nasazením do provozu. Návrh sledování dostupnosti, resp. chybovosti, jakož i výkonnosti musí být součástí projektových dokumentů (analýzy, technického designu, funkčního designu, implementační dokumentace) a zejména administrátorské a provozní dokumentace.

Návrh monitoringu vychází z doporučení dodavatele a je vypracován v součinnosti s VZP. Musí vycházet z popisu systémů, služeb a procesů aplikace, včetně návazností na ostatní systémy, a musí obsahovat zejména:

* způsob zjišťování stavu každé důležité komponenty / služby aplikace,
* návrh prahových hodnot nebo ukazatelů stavu,
* závažnost zjištěné události,  prioritu řešení události,  instrukce k řešení události.

Řešení monitoringu musí být navrženo tak, aby sledovaných událostí bylo co nejméně a sledování bylo proaktivní; události musejí včas upozornit na mezní stavy, aby bylo možné s předstihem zabránit výpadku služby, avšak nikoli za cenu inflace nevýznamných zpráv.

V HA aplikacích je nutné popsat režim, v němž jsou redundantní komponenty konfigurovány (loadbalance / failover) a určit závažnosti výpadků komponent a souvislosti kombinací těchto výpadků.

### 5.1.5. Požadavky na rozhraní pro monitoring

Všechny servery musejí na úrovni operačního systému umožňovat nasazení některého z agentů používaných dohledových nástrojů; spolu s agentem budou implementovány standardizované šablony s nastavenými prahovými hodnotami, které je možné na základě doporučení dodavatele upravit.

Všechna klíčová síťová zařízení musejí mít implementován protokol SNMP v. 3+ s možností hlášení událostí pomocí SNMP TRAP i GET, a s dostupnou MIB.

V případě monitorování pomocí logů (systémových, aplikačních apod.) musí být log v podobě cleartext souboru operačního systému v některém z obecně používaných formátů (Syslog, Common / Combined Log Format,…), resp. ve formátu Windows Event Log, případně lze použít dohodnutý formát. Logový soubor musí být lokální, tj. agent nemůže k logu přistupovat pomocí síťového protokolu na sdíleném prostředí. To nevylučuje vzdálené plnění logu. Jako nepřípustný pro automatizovaný monitoring je log v podobě průběžné databázové tabulky nebo pohledu.

Formát aplikačního logovacího souboru:

* oddělovačem je svislé lomítko „|“ (vertical bar, ASCII 124);
* žádné z polí zprávy by nemělo obsahovat diakritiku, pokud to není nutné např. z důvodu přenosu textu chybové zprávy z programu a jeho prostředí;  popis polí:
	+ datum a čas ve formátu '%Y.%m.%d %H:%M:%S'
	+ severity události podle výsledku operace: Critical, Major, Minor, Warning, Normal  Critical při fatální chybě, např. nemožnosti spustit operaci, kdy je nutný zásah v co nejkratší době;
		- Major při neúspěšném celkovém výsledku operace, např. neúspěchu posledního z pokusů o přenos, kdy je nutný zásah, např. manuální zpracování;
		- Minor při neúspěchu běhu operace, který bude opakován nebo jiné dílčí chybě, která nemusí znamenat neúspěch celé akce, a kdy je žádoucí kontrola průběhu
		- Warning při zjištění problémů u operace s úspěšným výsledkem nebo jiná upozornění, která vyžadují příležitostné prověření
		- Normal při úspěšném dokončení operace bez výhrad o proces, ke kterému se vztahuje událost, nepovinné
	+ objekt, který je zdrojem zprávy (např. program, název certifikátu, apod.), nepovinné o text zprávy, obsahující popis události a případné chyby

## 5.2. Zálohování a archivace

Všechna DC jsou zálohována jedním společným zálohovacím subsystémem (dále jen ZS).

### 5.2.1. Zálohovací systém

ZS je tvořen těmito komponentami:

* Řídící SW „Data Protector“.
* Cluster dvou serverů v oddělených lokalitách, na nichž je řídící SW provozován.
* HW pro ukládání zálohovaných dat, umístěný rovněž ve dvou různých lokalitách (DC), dostupný pomocí LAN a SAN infrastruktury. Jsou používány robotické páskové knihovny, které mohou být v případě potřeby doplněny o jiný HW (např. typu B2D), připojitelný pod řídící zálohovací software

Zálohování probíhá tak, aby byla respektována bezpečnostní zásada „3-2-1“ (tj. „důležitá data musí existovat 3x, ve 2 různých datových formátech, 1 kopie ve druhé lokalitě“) dle příslušné třídy aplikace.

### 5.2.2. Požadavky na aplikační celky z pohledu jejich zálohování:

Aplikace musí být navržena tak, aby:

* SW a HW komponenty aplikačních celků byly zálohovatelné technologiemi, které má VZP ČR v době nasazení aplikace a během jejího provozování k dispozici, v souladu s bezpečnostními standardy VZP ČR. Zálohovatelné musí být všechny SW komponenty a datové objekty potřebné pro činnost aplikace, a to s ohledem na předpokládané datové objemy, případné odstávky, propustnost potřebné infrastruktury a dobu potřebnou pro provedení záloh. Součástí dodávky aplikace musí být i analýza vývoje předpokládaných zálohovaných datových objemů.
* Umožňovala a podporovala datové odklady na jiná úložiště nebo zálohovací média. Musí tedy umět připravit data určená k odkladu/archivaci (např. umístit je do dohodnuté lokace, vhodně je pojmenovat, …) a vést o nich potřebnou evidenci po provedení odkladu. Musí

být také možné v případě potřeby takto odložená data po jejich obnově aplikaci opět zpřístupnit.

* Bylo možné omezit pravidelně zálohovaný datový objem (uspořádání dat do read-only datových objektů, které po jejich finální záloze sice mohou ležet na discích, ale již se dále nezálohují).
* Bylo možné identifikovat změny v datech, provedené od poslední zálohy
* Hodnoty parametrů RTO a RPO pro aplikační celky byly v souladu s platnými D+R a BC plány VZP ČR, a to i s ohledem na budoucí očekávané zálohované/obnovované datové objemy a datovou propustnost příslušné infrastruktury.

* Je-li pro tvorbu záloh třeba odstávka, součástí dodávky musí být potřebné nástroje, které umožní takové zálohy provádět automatizovaně.
* Jsou-li pro zálohování třeba nějaké další SW komponenty (přípravné scripty, programy třetích stran, …), musí být také součástí dodávky aplikace.
* Je-li pro zálohování některé části aplikačního celku potřeba příslušná zálohovací licence pro požadovaný typ zálohy (typicky pro online zálohy DB, Exchange, …), při nových dodávkách aplikačních celků ji zajišťuje VZP ČR, dodavatel aplikace však vždy musí v nabídkách a dalších dokumentech specifikovat, jaké typy záloh (s ohledem na námi používané technologie) budou požadovány.

*Vysvětlivky:*

*RTO = Recovery Time Objective … doba výpadku postižených služeb v případě obnovy*

*RPO = Recovery Point Objective … k jakému času lze data obnovit, která data bude třeba po obnově nahradit (datové změny od poslední zálohy), případně která nahradit nepůjdou*

## 5.3. Definice provozních parametrů služby/aplikace (SLA)

SLA a provozní parametry příslušné aplikace/domény budou součástí v technické specifikace příslušné komponenty (definované smluvně).

Využívané hodnoty:

**Provozní doba** **aplikace** – doba, kdy běží servery a aplikace

Režim provozní doby (7x24, 7x16, 5x16, 5x8)

**Podporovaná provozní doba** - doba, kdy provozní oddělení IT VZP zajišťuje personálně provoz aplikace

Režimy podporované provozní doby: 7x24, 7x16, 5x16, 5x8

**Doba podpory externím dodavatelem** - doba, po kterou je dostupná podpora dodavatele Režim doby podpory externím dodavatelem (7x24, 7x16, 5x16,5x10, 5x8)

**Servisní okno -** servisním oknem se rozumí vymezený časový rámec mimo provozní dobu služby na údržbu systému. Režim servisních oken

* Po 18:00 - 24:00 HW údržba
* Út 18:00 - 24:00 SW údržba
* St 18:00 - 24:00 HW údržba
* Čt 18:00 - 24:00 SW údržba

**Podpora Helpdesk** - standardní doba Helpdesku pro uživatele a řešitele -

Režim podpory Helpdesku

* Po – Čt 07:00 - 17:00
* Pá - 07:00 – 15:00

**Požadovaná dostupnost aplikace –** Dostupnost aplikace/služby koncovým uživatelům v procentech.

**Požadovaná doba odezvy -** časový interval mezi akcí uživatele a odezvou systému.

**Požadovaná spolehlivost** - střední doba mezi výpadky

Střední doba mezi obnovením služby po výpadku a vznikem nového výpadku dané služby. Uvádí se ve dnech.

## 5.4. Podmínky převzetí do rutinního prostředí a aplikační podpory

* Aplikace/služba je řádně otestovaná s příslušnou testovací dokumentací a akceptačními protokoly za jednotlivé druhy testů.
* Rutinní operace jsou plně automatizované (vyžadují pouze prvotní nastavení a následnou pravidelnou kontrolu), manuální operace jsou max. eliminovány (např. manuální kopírování dat v případě provozní chyby).
* Aplikace/služba je připravena k monitoringu všech funkcionalit, veškerého HW, SW a DB a je připravena k využití stávajících monitorovacích nástrojů.
* Aplikace/služba musí být předána dle standardního procesu předání aplikací do provozu včetně kompletní provozní dokumentace dle požadované struktury
* Aplikace/služba je dodána s kompletní dokumentací provozní i uživatelskou, včetně „Předávacích tabulek“ (přílohou standardů). K aplikaci/službě je dodán instalační postup a konfigurační příručka, podle kterých je možné jednoznačně aplikaci/službu instalovat a konfigurovat, bez jakýchkoliv manuálních zásahů.
* Po provedení instalace aplikace/služby dle dokumentace a instalačních postupů je stav aplikace/služby plně funkční, dle požadavků odběratele.
* Aplikace/služba je v době 1 měsíce od nasazení do produkčního prostředí v pilotním provozu, kdy se vyžaduje zvýšená podpora dodavatele
* Aplikaci/službu je po splnění a dodání výše uvedených bodů možné převzít do plného rutinního prostředí a následné aplikační podpory. viz přílohy:

P5\_předávací\_Tabulky\_produkčního prostředí

P5a\_předávací\_Tabulky\_testovací\_prostředí

## 5.5. Vazba na ITIL procesy

Aplikace musí být je zařazena ve VZP do standardních ITIL procesů

### 5.5.1. Definování veškerých eskalačních procedur u aplikace - správa HelpDesku/ServiceDesku

* Kritičnost aplikace
* Obnovení provozu
* Rozpoznání nestandardní situace
* Eskalační procedura

### 5.5.2. Zavedení aplikace do incident managementu

  Aplikace musí být zavedena do procesu Incident Managementu

### 5.5.3. Zavedení aplikace pod standardní řízení změn - change management

  Aplikace musí být zavedena do procesu Change Managementu, který má následující části:

* Požadavek a zadání změny o Schvalovací proces změny
* Realizace změny a předání úpravy aplikačního softwarového vybavení (dále zkratkou

ASW) podle pravidel release managementu (uvedeno v následující kapitole) o Nasazení změny ASW a akceptace v rámci procesu test managementu o Podle objemu a závažnosti zakázky je může být celý proces projektově řízen.

### 5.5.4. Zavedení aplikace do release plánů - release management

  Aplikace musí být zavedena do procesu Release Managementu

Ve VZP používáme toto rozdělení release:

* malý - malé změny, bez dopadu do integrace
* velký - velké funkční změny
* mimořádný – mimo termín release plánu – např. legislativou vynucené změny…

Pro každou komponentu ASW se v rámci dohody mezi dodavatelem a ICT VZP ČR nastaví release plán.

**6. Seznam příloh**

Příloha 1: P5\_předávací\_Tabulky\_produkčního prostředí

Příloha 2: P5a\_předávací\_Tabulky\_testovací\_prostředí

# Výjimky ze standardu:

## Integrace se stávajícím IS

Příloha 3: Integrace aplikace do IDM (Identity management)

Příloha 4: Integrace aplikace s CSČ (Centrální správa číselníků)

Příloha 5: Popis integračních vazeb prostřednictvím IPF a metodika realizace integračních vazeb

1. Pro vyhodnocení Transakčních logů je nezbytnou podmínkou zapnutí logování ESB, kdy vlastní vyhodnocení bude probíhat technologicky v nástroji, který propojí informace z Aplikačního auditního logu a logování ESB [↑](#footnote-ref-1)
2. Vyplnění atributů je povinné jen při volání mimo ESB [↑](#footnote-ref-2)
3. ID\_PARTNER slouží k logování pro GDPR, 101/2000 Sb. a ZoKB jako zdroj informaci o žádajícím subjektu při zpracování. Vlastní logování zpracovávaných osobních údajů (subjektů), kterých se daná transakce týká zajistí komponenta, která je původcem dané transakce [↑](#footnote-ref-3)