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 dokument 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	
1.07	23. 02. 2018	A. Žondecký	Úprava 3. kapitoly
1.08	7. 9. 2018	Michal Holinka	Revize integračních částí - pro účely CIS
1.09	26. 2. 2019	Jindřich Němec	Revize kapitoly Bezpečnostní standardy
1.10	11. 3. 2019	Juraj Boldiš	Úpravy v dokumentu, upřesnění logování
1.10.1	23. 5. 2019	Juraj Boldiš	Sloučeny změny s revizemi od OTP
1.10.2	12.6.2019	Juraj Boldiš	Úprava formátu
1.11	30.7.2019	Juraj Boldiš	Další revize k zapracování změn
1.11.1	18.10.2019	Jindřich Němec	Doplněna autentizace a autorizace
1.11.2	8.11.2019	Jindřich Němec	Finálizace změn v kapitolách kde je garantem OIKB

Obsah

1 Úvod

STANDARDY IS VZP - NIS

- **Představují -** soubor pravidel určených pro vytváření, rozvoj a využívaní IS VZP ČR.
- **Obsahují -** charakteristiky, metody, postupy a podmínky, které musí IT komponenty naplnit či dodržet, 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.** Výjimky zpracovává oddělení architektury, posuzuje je vlastník příslušného standardu VZP ČR, který je uveden u příslušné kapitoly. Schválení výjimky na základě posouzení schvaluje náměstek pro IT 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.

2 Architektonické a QA standardy

2.1 Aplikační – obecné standardy

Vlastník kapitoly: oddělení Architektury

- Aplikace má být navržena jako vícevrstvá, tyto vrstvy musí být jasně definovány a jejich rozdělení striktně dodržováno. Obvykle se aplikace skládá z těchto vrstev:
  Webová / presentační vrstva - uživatelské rozhraní -
  - Aplikační vrstva
  - Databázová vrstva
- Aplikační řešení musí být složeno z jednotlivých komponent s definovanými a oddělenými funkčnostmi, včetně rozhraní (API) jež funkčnosti zpřístupňují, bez duplicit a distribuované funkční logiky.
- Aplikační řešení by má být tvořeno ze sady relativně nezávislých modulů, aby změna v jednom z nich neznamenala (podstatný) zásah do zbývajících modulů. Moduly jsou v ideálním případě samostatně (autonomně) nasaditelné (upgradovatelné).
- Aplikace musí mít deklarovatelným způsobem ošetřeny architektonické aspekty: škálovatelnost a flexibilita a to zejména **umožněním horizontálního škálování;**
- Součástí návrhu aplikačního řešení a realizace je požadován kapacitní a výkonnostní sizing systému s výhledem na 5 let.
- Aplikace musí splňovat požadavky na zálohování a obnovu popsané níže.
- Aplikace/ Řešení musí podporovat mechanismy pro archivaci dat a jejich případnou obnovu
- Aplikace musí respektovat již v návrhu požadavky na bezpečnost a soulad (compliance), viz kapitola 4 Bezpečnostní standardy.

2.1.1 Třídy Aplikací

Aplikace a aplikační řešení jsou z pohledu kritičnosti provozu kategorizovány do následujících tříd:

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).

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.

2.2 Integrační a komunikační standard

Vlastník kapitoly: oddělení architektury

- Komunikace mezi aplikacemi a integrace musí respektovat následující pravidla: Komunikace je v zásadě asynchronní (synchronní komunikace pouze ve výjimečných odůvodněných případech);
- Komunikace musí být odolná proti výpadku jedné strany
- Komunikace maximálně omezuje využívání mechanismů:

  - distribuovaná transakce
  - dvoufázové potvrzení transakce (two-phase- commit);
- Komunikace dodržuje zásady idempotence[1], tam kde je to možné.
- Veškeré vazby systému na ostatní systémy jsou formou volné vazby (loosely coupled), doporučeným mechanizmem aplikační komunikace je využití messagingu, případně synchronních REST služeb.
- Pro přenos souborů (MFT) a datových objektů větších než 2MB se využije souborový přenos.
- Pro datovou integraci se využijí nástroje ETL, případně nástroje pro Event Streaming .
- Pro implementaci nových veřejných rozhraní (API) upřednostňovat REST v3.0 (HATEOAS[2]).
- Spojení mezi stávajícími systémy VZP provádět přes integrační platformu (ESB).
- V maximální možné míře je nutno využívat stávajících již implementovaných aplikačních služeb nabízených v infrastruktuře VZP.
- 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 (batch, ETL, MFT) 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 8.1 Integrace se stávajícím IS.

2.3 Vývojové standardy

Vlastník kapitoly: OAVRZ

2.3.1 Použité vývojové nástroje pro interní vývoj aplikací:

- Funkční analýza a design: Enterprise Architekt, MS Word, Balsamiq Mockups
- Technický design-aplikační logika: Visual Studio 2015/2017
- Technický design-datový design: Visual Studio 2017 Database Tools (MSSQL / Oracle)
- Technický design-integrační procesy: OpenAPI / AutoRest (Enterprise Architect, MS Word)
- Správa verzí: Visual Studio Team Services (Git), Gitlab
- Vývoj aplikací: Visual Studio 2015/2017, Visual Studio Code, SQL Server Management Studio, XCode / Android Studio, SOAP UI, Postman
- Migrace a deployment aplikací: Azure DevOps

2.3.2 Vývojová a testovací prostředí

Vyvíjená aplikace musí mít definována minimálně prostředí:

- Samostatné prostředí určené konkrétnímu vývojáři
- prostředí určené pro ověřovací testy v rámci vývoje, preferováné je, aby nasazování na tato prostředí probíhá automaticky
- prostředí určené pro akceptační test garanty aplikací, nasazení na tato prostředí je řízeno pověřeným vedoucím testování (určeným vedoucím testovacího oddělení)
- Verzování vývoje

[1] (https://en.wikipedia.org/wiki/Idempotence)
[2] http://restcookbook.com/Basics/hateoas/

- Vyvíjená aplikace bude verzována pomocí tzv. sémantického verzování[3]

2.4 Testovací standardy

Vlastník kapitoly: OTP Oddělení testování

- 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/pseudonymizovaných datech (součástí řešení jsou nástroje pro anonymizaci/pseudonymizaci testovacích dat)
- Musí být zajištěna jednotná anonymizace/pseudonymizace dat integrovaných aplikací v rámci testovacího prostředí

Typy požadovaných testů pro předání do provozu IT

Vývojové testování			
Název testu	**Provádí**	**Vstupy**	**Výstupy**
unit test assembly test funkční test test výjimek	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
Systémové testování			
Název testu	**Provádí**	**Vstupy**	**Výstupy**
smoke test funkční test test výjimek integrační test	testeři dodavatele komponenty společně s testery VZP ČR[4]	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
Nefunkční testy			

[3] https://semver.org/lang/cs/

[4] Společně s testery VZP znamená poskytnutí přiměřené součinnosti VZP k provedení a přípravě testu tam kde je to věcně nezbytné.

Název testu	Provádí	Vstupy	Výstupy
zátěžový test[5] stress test	testeři dodavatele komponenty společně s testery 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
Backup a recovery test	Administrátoři VZP ČR	Postup zálohy a postup obnovení. Testovací scénáře ověřující základní funkčnosti po záloze a obnovení	Záznam ověření provedení obnovy ze zálohy.

Bezpečnostní testy			
Název testu	**Provádí**	**Vstupy**	**Výstupy**
bezpečnostní test	testeři OBIT VZP ČR	Identifikace komponent k testování (dodavatel a VZP ČR)	Výsledky testu
penetrační test (u Internet facing aplikací / systémů)	penetrační testování zajišťuje nezávislý subjekt (subdodávka), náklady nese dodavatel	Identifikace komponent k testování (dodavatel a VZP ČR), návrh rozsahu penetračního testu (dodavatel, VZP ČR)	Výsledky 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

Vlastník kapitoly: OAVRZ

[5] Pro zátěžové testy prefreuje VZP ČR nástroj jMeter (https://jmeter.apache.org/)

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	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

	řešení a způsob, jak nového řešení dosáhnout ve vazbě na stávající stav.	
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 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.	Aplikační architektura Integrační architektura Datová architektura Technologická architektura Technické předpoklady, omezení Postup implementace a migrace
Bezpečnostní dokumentace[6]	Popis integrace do sítě VZP ČR s ohledem na umístění komponent v rámci segmentace komunikační sítě (dle DC zón a zón Perimetru). Popis potřeb a návrh řešení s ohledem na	Síťová bezpečnost

[6] Pokud informace požadované bezpečnostní dokumentací uvedl zpracovatel v rámci jiné dokumentační oblasti, pak je v bezpečnostní dokumentaci řešeno odkazem.

	komunikaci mimo síť VZP ČR. Výčet služeb poskytovaných do veřejné a vnitřní sítě.	
	Popis mechanismu autentizace a autorizace uživatelů. Napojení na centrální autority autentizace a autorizace. Napojení na IDM/EIM.	Autentizace a Autorizace uživatelů
	Výčet použitých účtů a rolí (včetně účtů a rolí dodaných s aplikací nebo systémem nebo nebo vytvořených na základě zadání VZP ČR). Identifikace, zda je účet nebo role vytvořena lokálně, nebo převzata z centrální autority, zda se jedná o privilegovaný účet nebo roli, popis využití účtu nebo role. Matice rolí, která identifikuje nežádoucí kombinace systémových rolí (kombinace, které mohou zapříčinit zneužití přidělených oprávnění při kumulaci rolí)	Uživatelské a servisní účty
	Identifikace a popis informačních aktiv se kterými systém nebo aplikace pracuje a klasifikace informačních aktiv. V případě osobních a citlivých údajů popis kategorií subjektů údajů a kategorií osobních údajů, plánované lhůty pro výmaz jednotlivých kategorií údajů, účelu zpracování a právního důvodu zpracování.	Výčet primárních aktiv typu informace
	Při zpracování osobních informací je součástí bezpečnostní dokumentace analýza „Vliv zamýšlených operací zpracování na ochranu osobních údajů“, tedy analýza rizik a dopadů zpracování dat a dokumentů.	Vliv zamýšlených operací zpracování na ochranu osobních údajů
	Popis integračních vazeb (vazby na další komponenty IS VZP ČR nebo státní správy) z pohledu bezpečnosti a to specificky se zaměřením na využitý komunikační framework, popis a klasifikaci přenášených informačních aktiv, mechanismy autentizace, autorizace a auditu, způsobu zabezpečení vč. specifikace použitých šifrovacích mechanismů.	Integrační vazby

	V případě, že systém nebo aplikace využívá v rámci kryptografických opatření privátních klíčů, pak jsou součástí dokumentace informace o uložení a zabezpečení privátních klíčů. Z provozní dokumentace musí být zřejmé, kde a za jakým účelem jsou privátní klíče využity. V případě, že systém, nebo aplikace využívá v rámci kryptografických opatření certifikátů vydaných CA VZP ČR (technologický certifikát), pak je nutné zajistit, aby byl dokumentován postup výměny certifikátu v provozní dokumentaci. Rovněž musí být popsáno, jakým způsobem je procesně zajištěno, že nedojde k přerušení činnosti aplikace nebo systému díky expiraci certifikátu. Z provozní dokumentace musí být zřejmé, kde a za jakým účelem jsou certifikáty využity.	Kryptografická opatření
	Výčet zaznamenávaných bezpečnostních událostí, včetně popisu formátu, místa uložení a retence.	Bezpečnostní logování
	Podrobný plán obnovy systému. V případě, že systém využívá asymetrické kryptografie, pak jsou součástí dokumentace informace o zajištění zálohování a obnovy privátních klíčů.	Plán kontinuity činností
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/pseudonymizaci 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 Obecné zásady

Standardem pro provoz aplikací je virtualizovaná infrastruktura. Virtualizace může být realizována formou virtuálních serverů, kontejnery či přímým hostingem funkcí.

Instalace aplikace na bare-metal HW je možná pouze po schválení výjimky ze strany OTP a Oddělení architektury.

Infrastruktura provozovaná formou služby (public cloud) není povolena.

3.2 HW

Vlastník kapitoly: OTP OSI

3.2.1 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.

Standardem pro připojení fyzických serverů do sítě LAN v datových centrech je:

- Management console konzole, 1x1GE, access
- Management interface, 2x1GE, acces, active-standby
- Datový interface, 2x10GE, trunk, active LACP

On Premise SAN infastruktura

V jednotlivých datových centrech jsou 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 zařízení (páskové knihovny, B2D zařízení) a zmíněná disková pole. Tato SAN síť využívá u všech významných komponent minimálně 2 FC rozhraní pro zajištění vysoké dostupnosti.

3.2.1.1 Podmínky pro on – premise infrastrukturu podle Třídy Aplikací

Třída A

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

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).

3.3 Sítě

Vlastník kapitoly: OTP OSS

3.3.1 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).

3.3.2 QoS (QUALITY OD 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

3.3.3 Datová centra

Fyzická topologie síťové vrstvy v každém z datových center VZP ČR je tvořena dle architektury Spine and Leaf. Logická síťová vrstva je centrálně řízena pomocí clusteru controllerů. Jedná se o aplikačně řízenou infrastrukturu (Application Centric Infrastructure - ACI), která umožňuje 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.).

VZP ČR používá technologii Cisco ACI.

3.3.3.1 Architektura datových center

Z pohledu architektury se obě datová centra chovají jako jedno logické datové centrum, dále jen NDC – Nové Datové Centrum. NDC je v prostředí ACI vytvořeno několika tenanty (virtuálními prostředími). Pro zajištění sdílení infrastrukturních a společných služeb je využit tenant common.

Přehled použitých tenantů (prostředí):

- Sdílené služby (common) – služby sítě, AAA, management, dohled, ostatní společné síťové služby, propojení do uživatelské sítě VZP net.
- Administrativní/Management prostředí (ADM) – out-of-band management připojení, management rozhraní
- Produkční prostředí (PRO) – produkční aplikační celky
- Testovací prostředí (TSTxx) – testovací prostředí TST01 – TST12. Každé testovací prostředí je samostatným tenantem, tedy až 12 tenantů.

Produkční a testovací prostředí NDC je rozděleno do aplikačních celků. Každý aplikační celek je tvořen samostatným aplikačním profilem. Aplikační celek se typicky skládá z jednotlivých EPG (End Point Group) reprezentujících vrstvu aplikace:

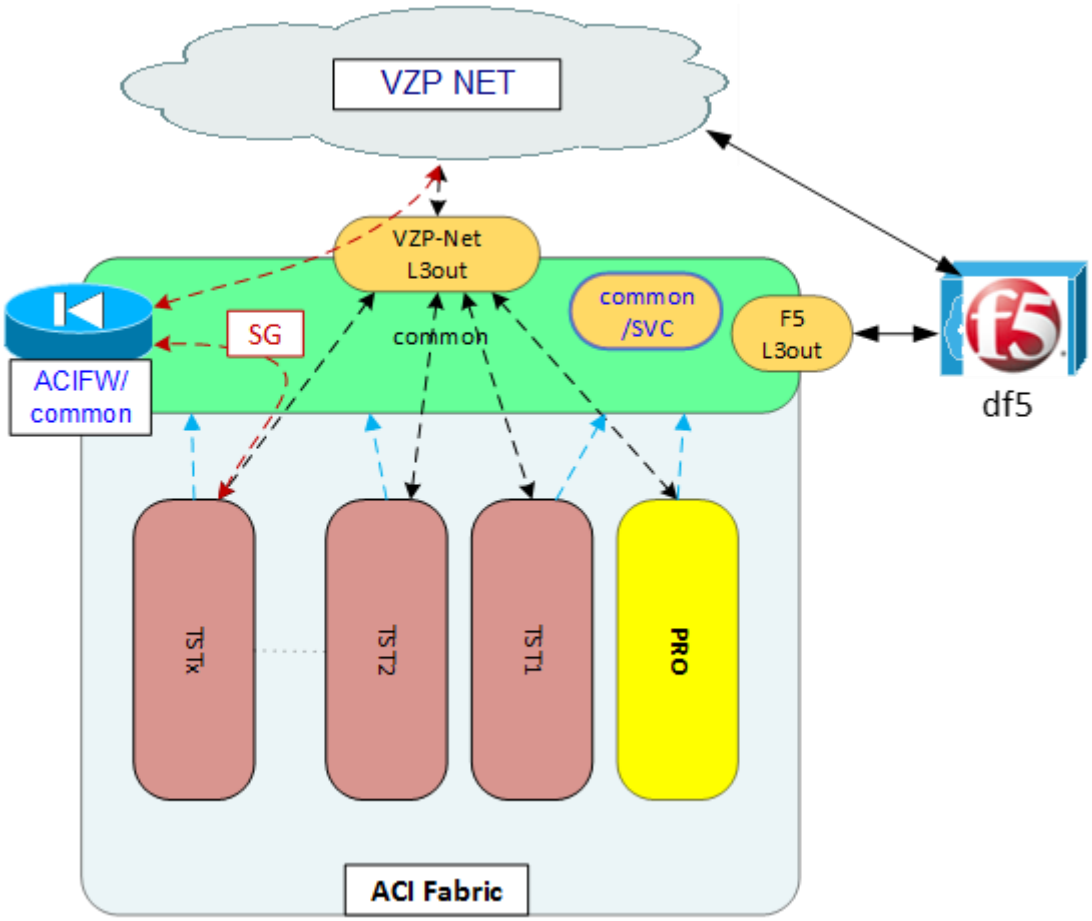
- Webová (Prezentační) vrstva
- Aplikační vrstva (APP EPG)
- Databázová vrstva (DB EPG)
- HeartBeat vrstva

- Aplikační profil (Application Profile) je množina EPG a kontraktů/filtrů, které dohromady tvoří pravidla pro komunikaci v rámci vybrané aplikace.
- EPG je logická skupina serverů/aplikací/koncových zařízení, pro kterou jsou definovány jednotlivé politiky. V rámci EPG je standardně povolena veškerá komunikace. Mezi jednotlivými EPG je standardně veškerá komunikace zakázána a povolená komunikace je stanovena pomocí konraktů (contracts).
- Kontrakty (contracts) je skupina politik, která definuje potencionální komunikaci mezi jednotlivými EPG. Kontrakt je tvořen filtry (filters), které definují specifické protokoly a porty, které jsou povoleny v komunikaci mezi EPG.

Bezpečnostní oddělení (řízení provozu) na síťové vrstvě je zajištěno následujícími prostředky:

- East-West provoz – komunikace v rámci tenanta uvnitř ACI prostředí – je řízena pomocí standardních contractů mezi jednotlivými EPG.

- East-West provoz – komunikace mezi tenanty uvnitř ACI prostředí –probíhá výjimečně a je řízena pomocí standardních kontraktů mezi jednotlivými EPG nebo ve specifických odůvodněných případech je využit servisní graf obsahující firewall.
- North-South provoz – komunikace ze sítě VZP (administrátoři) do tenantů NDC –probíhá přes L3 out spojení, kde bude vytvořen servisní graf se zařazením firewallu pomocí PBR (Policy Based Redirect).
- North-South provoz – komunikace ze sítě VZP (uživatelé) do tenantů NDC –probíhá přes L3 out spojení přes loadbalancer F5 bez servisního grafu, tj. bez firewallu.



Obrázek: Tenanti a komunikace v ACI a mimo ACI

3.3.4 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.

3.3.5 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

3.4 OS

Vlastník kapitoly: OTP OSSM

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

3.4.1 OS pro aplikace třídy A

- Red Hat Enterpise Linux, Oracle Linux, CentOS (verze 7 a vyšší)
- MS Windows Server 2016

3.4.2 OS pro aplikace třídy B

- Red Hat Enterprise Linux, Oracle Linux, CentOS (verze 7 a vyšší)
- MS Windows Server 2016

3.4.3 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 6.5 Enterprise a vyšší, Oracle VM 3.4 a vyšší.

Řízení Virtuálních serverů - správa VMs na VMWare nástrojem VMWare vCenter Server 6.5 Standard a vyšší.

Pro zajištění vysoké dostupnosti aplikací třídy A pro a realizaci DRP plánu slouží technologie VMware DRS a HA cluster, případně VMware SRM.

Pro aplikace třídy A využívající softwarové produkty Oracle bude použita virtualizace Oracle VM.

U aplikací třídy B lze použít i další virtualizační technologií:

- KVM (Kernel-based Virtual Machine)

3.4.4 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.

3.5 Middleware

Vlastník kapitoly: OTP OSAD

3.5.1 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.

3.5.2 Webové servery

Výčet typů WS využívaných v IS VZP:

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

3.6 Virtualizovaná infrastruktura pro hostování aplikací

Vlastník kapitoly: OTP OSAD

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

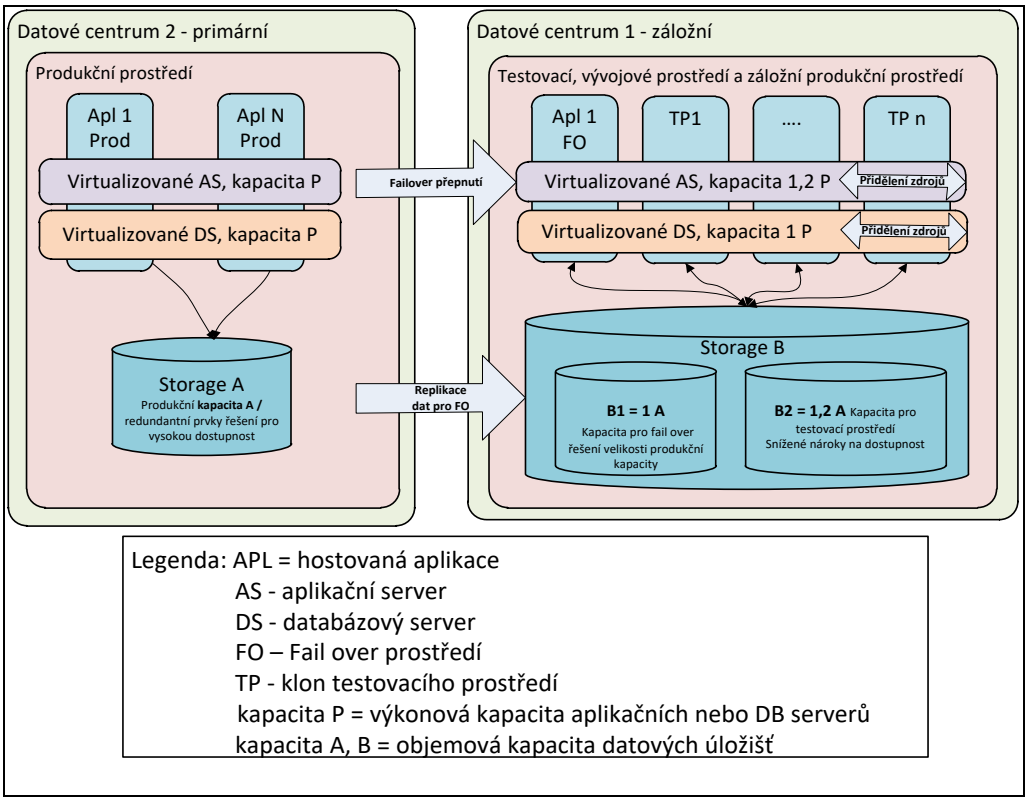
Název služby	Popis
Server s OS	OS Windows nebo Linux (viz kap. 3.3 OS)
Aplikační server	OS Windows nebo Linux aplik. serveru Oracle Weblogic Suite
Databázový server Oracle	OS Linux, Oracle dB EE + RAC + partitioning
Databázový server MS SQL	OS MS Windows, MS SQL Server v edici Enterprise

3.7 Deployment aplikací provozovaných on-Premise do prostředí v DC VZP

Vlastník kapitoly: OTP OSAD

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.
- Kapacita úložiště Storage B musí být 2,2 násobkem kapacity úložiště produkčního prostředí Storage A
- Kapacita HW serverů pro databázovou a aplikační vrstvu musí být výkonově dimenzována jako 1,2 násobek produkčního prostředí (měřeno součtovým počtem jader, velikostí operační paměti virtuálních serverů a diskových úložišť pro aplikační a databázovou vrstvu). Redundance komponent není nutná.



3.8 Datové a databázové služby

Vlastník kapitoly: OTP OSAD

3.8.1 Databázové technologie

Standard	Popis
Oracle DB EE v nejnovější podporované verzi, včetně databázových options	Pro aplikace třídy A nebo B.
MS SQL EN/STD min. verze 2014, X64bit, standalone/cluster	Podpůrné služby a pro aplikace v třídě B. V odůvodněných případech je možné použít i pro aplikace třídy A.

3.8.2 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 nežádoucího 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.

4 Bezpečnostní standardy

Vlastník kapitoly: OKIB

4.1 Dodržování legislativních požadavků

Dodávaný systém, nebo aplikace, je v souladu (po technické / procesní stránce poskytuje takové funkcionality, které VZP ČR umožní být v souladu) s níže uvedenými zákony a nařízeními:

4.1.1 Autorský zákon

Zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů, v platném znění.

4.1.2 ZOKB

Zákon č. 181/2014 Sb. (Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (Zákon o Kybernetické bezpečnosti) v platném znění (zkratka ZoKB) a související Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) a to především v oblastech:

- zajištění průběžného a včasného odstraňování zranitelností systému, nebo aplikace po celou dobu podpory (subjekt odpovědný za správu systému, nebo aplikace vždy zajišťuje odstraňování zranitelností dle PŘ 2018/13 čl. 7);
- implementace vhodného způsobu řízení přístupu k informačním aktivům na základě rolí vč. autentizačních a autorizačních procesů;
- implementace logování systému, nebo aplikace.

4.1.3 GDPR

„Nařízení Evropského parlamentu a Rady č. 679/2016 ze dne 27. 4. 2016“ (zkratka GDPR) a to především v oblastech:

- implementace procesů / datových modelů umožňujících a podporujících zajištění omezení doby zpracování (odstranění osobních údajů fyzických osob, které již nemají z hlediska VZP ČR další účel zpracování a kterým současně již uplynula stanovená doba pro uchování osobních údajů)
- implementace logování přístupu k příslušným informačním aktivům na aplikační úrovni
- implementace podpory mechanismů umožňujících snadné předání údajů zpracovávaných v příslušné aplikaci ve strojově čitelné podobě jinému správci
- ve spolupráci s VZP ČR zajistit provedení analýzy „Vliv zamýšlených operací zpracování na ochranu osobních údajů“ (Data Protection Impact Assessment - DPIA)

4.2 Dodržování obecných standardů a doporučení

V rámci dodávky/vývoje je doporučeno dodržování obecně platných standardů uvedených níže. Výjimky nebo odchylky od uvedených standardů musejí být předem schváleny VZP.

- Center for Internet Security Benchmark;
- Application Security Verification Standard;
- 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)*).

4.3 Minimum běžících a instalovaných služeb

Jsou nainstalovány a spuštěny pouze takové služby, které jsou pro provoz systému / aplikace nezbytné.

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…);
- použití služeb se známou zranitelností, která není výrobcem opravena nebo je neopravitelná;
- použití služeb bez podpory výrobce (Out Of Life).

4.5 Synchornizace času

Systém provádí synchornizaci času s NTP servery VZP ČR (ntp1.vzp.cz, ntp2.vzp.cz, ntp3.vzp.cz) nejméně jednou za 24 hodin.

4.6 Kryptografie

4.6.1 Požadavky na kryptografické algoritmy

Kryptografické algoritmy musí splňovat doporučení NÚKIB platné ke dni 28. 11. 2018. Dokument lze získat ze stránek https://www.govcert.cz/cs/doporuceni-v-oblasti-kryptografickych-prostredku/.

4.6.2 Požadavky na ochranu privátního klíče

- 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.

4.6.3 Požadavky na CA / PKI

- Služba, které přísluší v roli interní certifikační autority VZP ČR vydávat na základě, certificate signing request‘ (CSR) certifikáty (technologické nebo osobní) musí být schopna kromě věcí obvyklých, jako je zajištění bezpečného vydávání těchto certifikátů, jejich bezpečná distribuce, omezení platnosti na max. 2 roky umožnit i jejich zneplatnění za pomoci vystavení tzv. ‚certificate revocation list‘ (CRL);
- systémy, nebo aplikace využívající certifikátů vydaných touto certifikační autoritou musí být schopny reagovat na změny v CRL;
- pro každé řešení v roli CA / PKI VZP ČR musí být zajištěno, že jsou vydané certifikáty evidovány a před dobou expirace certifikátu je vlastník upozorněn na blížící se expiraci certifikátu, toto platí **zejména pro certifikáty technologické** (upozornění musí být odesíláno min. tři měsíce předem vlastníkovi aplikace a procesně musí být vynuceno ověření, že došlo k výměně certifikátu);
- dodavatel nemůže bez svolení pro svoje řešení využívat neschválenou CA / PKI, případně řešit zabezpečení tzv. ‚self-signed certifikáty‘a preferenčně musí využít centrálná CA / PKI VZP ČR.

4.7 Komunikace s veřejnou sítí

4.7.1 Systémy, nebo aplikace, které publikují služby do veřejné sítě (inbound)

Všechny On-Premise systémy, nebo aplikace, které publikují služby do veřejné sítě (např. poskytující B2B API, webové prezentace apod.) jsou:

- umístěny ve vyhrazeném síťovém segmentu (vnitřní perimetr), který je dohledován IDS/IPS řešením a má omezené možnosti komunikace do vnitřní sítě;
- zapojeny tak, že je aplikačními firewally prováděna inspekce provozu.

4.7.2 Komunikace do veřejné sítě (outbound)

Všechny On-Premise systémy, nebo aplikace, které potřebují pro zajištění svého provozu komunikovat s veřejnou sítí, kromě systémů, nebo aplikací poskytujících základní infrastrukturní služby typu DNS, NTP, e-mail gw pro veřejnou síť, Proxy (vč. schválených výjimek) s veřejnou internetovou sítí nekomunikují přímo, ale pro komunikaci s veřejnou sítí využívají proxy server (proxy server zajišťuje terminaci šifrovaného kanálu a inspekci provozu).

4.7.3 SMTP komunikace s veřejnou sítí

- SMTP brána, která komunikuje s veřejnou sítí, musí:
- být umístěna ve vyhrazeném síťovém segmentu (vnitřní perimetr), který je dohledován IDS/IPS řešením a má omezené možnosti komunikace do vnitřní sítě;
- identifikovat nevyžádané emaily (pomocí heuristiky, RBL, reputace odesílatele, nebo kombinací těchto mechanismů) a aplikovat na ně příslušné politiky (např. odmítnutí doručení, označení zprávy jako nevyžádané apod.);
- podporovat šifrování emailové komunikace mezi emailovými servery (SMTPS);
- zabránit potenciálnímu spoofingu emailové komunikace (SPF);
- Identifikovat malware a zabránit jeho doručení (využívat sandboxingu, nebo antivirového řešení).

4.8 Řízení přístupu

4.8.1 Autentizace a autorizace při přístupu k systémum, nebo aplikacím VZP ČR z interní sítě VZP ČR

4.8.1.1 V případě koncových uživatelů (pracovníků VZP ČR, kontraktorů VZP ČR):

- správa identit koncových uživatelů je uchovávána v nástroji pro správu a ověřování identit uživatelů, administrátovů a aplikací, kterým je centrální AD VZP ČR;
- musí být zajištěno řízení přístupových oprávnění k jednotlivým IS VZP ČR **na základě přístupových skupin a rolí** v nástroji pro řízení přístupových oprávnění, kterým je IDM (Identity Management Systém) VZP ČR;
- koncový uživatel (v rámci vnitřní sítě VZP ČR) musí vždy prokazovat svoji identitu směrem k aplikačnímu uživatelskému front-endu principem SSO, kdy **autentizace je zajištěna transparentně** (bez interakce uživatele);
- interaktivní autentizace koncového uživatele probíhá pouze do operačního systému;
- **Autentizace** koncového uživatele:
    - musí probíhat proti centrálnímu AD VZP ČR.
- **Autorizace** koncového uživatele:
    - je řízena IDM , ve kterém jsou přístupová oprávnění a skupiny definovány.

4.8.1.2 V případě komponent IS VZP ČR (API a dalších technologických rozhraní):

- Musí být zajištěno řízení přístupů k jednotlivým IS VZP ČR.

Autentizace komponent IS v rámci SOA (v souvislosti s prokázáním identity komponenty IS musí být využito alespoň jednoho z níže uvedených způsobů:

  - PKI VZP ČR. Všechny komunikující komponenty IS musí při ustanovení komunikace využít certifikát vydaný centrální certifikační autoritou VZP ČR (CA VZP ČR). Ověření platnosti certifikátu (podpis CA, rozsah platnosti, identita serveru/klienta) je prováděno na obou stranách, resp. klientem služby i konzumentem služby (mutual authentication);
  - případně s využitím podpůrné infrastruktury IdP a IdS (tiketů/tokenů, SAML/JWT) existující v době realizace zakázky.

- **Autorizace** komponenty IS v rámci SOA (musí být zajištěna alespoň jedním z níže uvedených způsobů):
  - Využitím atributu „DN“ certifikátu využitého pro autentizaci komponenty, na základě předaného „DN“ volaný systém ověří (LDAP nebo lokální úložiště), zda volající systém má autorizaci pracovat s API systému volaného (preferovaná varianta);
  - API key (tato varianta musí být schválena VZP ČR);
  - srovnáním fingerprintu konkrétního certifikátu klienta služby (import veřejného certifikátu klienta služby), tato varianta musí být schválena VZP ČR;
  - podepsáním zprávy (výměna veřejných klíčů mezi komunikujícími aplikacemi), tato varianta musí být schválena VZP ČR;
  - získáním informace o autorizaci pro danou operaci z externího pro to určeného řešení (LDAP/AD apod), tato varianta musí být schválena VZP ČR.

4.8.2 Autentizace a autorizace při přístupu k systémům, nebo aplikacím VZP ČR z veřejné sítě

4.8.2.1 V případě koncových uživatelů (klientů VZP ČR):

- správa identit koncových uživatelů musí být uchovávána a řízena v nástroji pro správu a ověřování identit uživatelů (EIM – Externí Identity Management), tj.není jím centrální AD VZP ČR;
- musí být zajištěno řízení přístupových oprávnění k jednotlivým IS VZP ČR na základě přístupových skupin a rolí v nástroji pro řízení přístupových oprávnění – IDM (Identity Management Systém) .
- **Autentizace** koncového uživatele.
  - musí probíhat proti EIM.
- **Autorizace** koncového uživatele:
  - je řízena IDM, ve kterém jsou přístupová oprávnění a skupiny definovány.

4.8.2.2 V případě koncových uživatelů (pracovníků VZP ČR, kontraktorů VZP ČR):

- Koncový uživatel VZP ČR přistupuje do vnitřní sítě VZP ČR z veřejné sítě Internet vždy prostřednictvím VPN VZP ČR. Není proto důvod, aby byly služby pro tento typ koncové uživatele vystaveny přímo do Internetu. To platí rovněž pro služby využívané uživateli s privilegovanými oprávněními - administrátory.
- **Autentizace**:
  - uživatelským účtem spravovaným v AD VZP ČR a osobním certifikátem vydaným CA VZP ČR.
- **Autorizace**:

4.8.3 viz. 4.8.1.1 Propagace identity uživatele ke koncovým službám

- Identita konkrétního uživatele je ověřena z front-endu nebo API aplikace a **vždy** propagována až ke koncovým službám přes všechny technologické vrstvy IS VZP ČR a to především z důvodu určení původce transakce a jeho pozdější identifilaci v příslušném aplikačním logu.

4.8.3.1 Propagace identity pro SOAP Webové služby:

Bude využit standardní UserName token s uživatelským jménem koncového uživatele. Token nebude obsahovat žádné heslo a bude odesílán v rámci WS-Security hlaviček SOAP požadavku. Viz následující příklad:

```
<?xml version="1.0" encoding="UTF-8"?>

<soap:Envelope xmlns:soap="http://.../soap/envelope/">

 <soap:Header   xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">

  <wsse:Security>

    <wsse:UsernameToken wsu:Id="UsernameToken-484-624e-938a-a986-a5e8717dcb3d">

      <wsse:Username>melich99</wsse:Username>

    </wsse:UsernameToken>

  </wsse:Security>
   . . . . . .

  </soap:Header

  <soap:Body>

   . . . . . .

  </soap:Body>

</soap:Envelope>
```

4.8.3.2 Propagace identity pro RESTové služby

Pro propagaci identity na REST API bude využita hlavička aplikačního protokolu HTTP. Vzhledem k tomu, že využití standardní hlavičky *Authorization* pro čistou propagaci identity bývá matoucí, bude využita custom hlavička *iv-user.* Viz následující příklad:

```
GET /serverapi/v1/documents/12332222777/content http 1.1

host: esb.ecm.vzp.cz

iv-user: melich99
```

4.8.4 Ochrana hesel a politika hesel

- Hesla nesmí být uchovávána v čitelné podobě v dávkových souborech, automatických přihlašovacích skriptech, makrech, v nechráněných souborech a všude tam, kde by mohlo dojít k jejich odhalení.
- Systém, nebo aplikace, musí zajistit ochranu hesel a vynucovat politiku hesel v souladu s požadavky ZoKB, resp. Vyhlášky 82/2018.

4.8.5 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).

- Po definovaném počtu neúspěšných pokusů (5 pokusů) o přístup musí dojít k automatickému uzamčení příslušného účtu. Tento požadavek se nevztahuje na systémové účty, kde by mohlo uzamčení účtu způsobit provozní problémy. Opětovné odemknutí je v kompetenci Administrátora systému nebo aplikace. Mechanismus musí být navržen tak, aby nedošlo k hromadnému zamykání a tím odepření služby.

4.8.6 Omezení přístupů ke službám ve vnitřní síti VZP ČR

Systémy, nebo aplikace, publikují do sítí, ze kterých k němu přistupují koncoví uživatelé, výhradně služby, které jsou koncovým uživatelům určené. Jiné služby (např. služby zajišťující integraci s jinými systémy) nesmí být nikdy ze sítí, ve kterých pracují koncoví uživatelé, dostupné.

4.8.7 Zobrazení varovného hlášení

V případě systému, nebo aplikace, kdy uživateli jsou pracovníci VZP a systém, nebo aplikace obsahuje chráněné informace, musí být uživatelům před dokončením procesu autentizace zobrazeno varovné hlášení, které je informuje o důsledcích jejich aktivit. Toto hlášení musí uživatele varovat, že neoprávněný pokus o přihlášení, nebo zneužití takového přístupu může vést k pracovně právnímu postihu a/nebo trestnímu stíhání a dát jim možnost proces autentizace ukončit.

Varovné hlášení musí obsahovat následující text: "*Veškerá práva k systému a údajům v něm obsažených jsou vyhrazena ve prospěch VZP ČR. Vstup do tohoto systému je umožněn pouze na základě autorizovaného přístupu a při dodržování příslušných bezpečnostních pravidel. Jakékoli nakládání, přenášení nebo jiné zpracování údajů obsažených v tomto systému v rozporu s pokyny nebo souhlasem VZP ČR jsou zakázány. Aktivity v tomto systému jsou monitorovány.*".

4.9 Ochrana informačních aktiv

Systém, nebo aplikace, musí zajistit:

- kompletnost a platnost dat při zaručeném zpracování pouze autorizovanými systémy a uživateli;
- nesmí umožnit neautorizovaný zásah do evidovaných informací / dat.

4.9.1 Klasifikační schéma informačních aktiv

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

- **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,
- **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,
- **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.

Mezi **chráněné informace** patří:

- **osobní údaje** - jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.
- **zvláštní kategorie osobních údajů** - osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě

subjektu údajů a genetický údaj subjektu údajů; do zvláštní kategorie osobních údajů spadá biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.

Tam, kde je to možné, je provedena anonymizace subjektů přiřazením jedinečného identifikátoru, který s sebou nenese žádná osobní data.

4.9.2 Data v klidu (Data at Rest)

- Pokud data obsahují chráněné informace, pak musí být při uložení šifrovány (v databázích a datových skladech, na souborovém systému, na páskách a dalších výměnných médiích, v mobilních zařízeních apod.).
- Pro případ zničení primárních dat musí být data zálohována a archivována. Záložní kopie musí být umístěny v geograficky vzdálené lokalitě, nebo tak, aby nehrozilo současné zničení medií a zdrojových dat.
- Zálohovaná data se musí podepisovat a používat mechanismus kontrolního součtu.
- Musí být nastaven proces pro bezpečnou likvidaci již nepotřebných dat a to tak, aby informace nešlo obnovit.

4.9.3 Data v pohybu (Data in Transfer)

- Pokud data obsahují chráněné informace, pak musí být během přenosu po síti šifrovány.
- je doporučeno data obsahující chráněné informace podepisovat.

4.9.4 Data při zpracování použití (Data in Use)

- Přístup k informacím musí být řízen na základě přístupových oprávnění pro jednotlivé uživatele a jednotlivá aktiva.
- Je uplatňován princip "*need to know",* do produkčních prostředí, která obsahují chráněné informace nemají např. přístup pracovníci vývoje.
- V případě, že informace obsahují osobní, nebo zvláštní kategorie osobních údajů, musí být operace (přístup a změna) nad těmito informacemi logovány.
- V neprodukčních prostředích (vývojová a testovací prostředí) nesmí být využívány chráněné informace.
- Informace v neprodukčních prostředích jsou anonymizovány, kdy Anonymizací se rozumí taková úprava, po které nelze údaje vztáhnout k určenému nebo určitelnému subjektu údajů.

4.9.5 Antimalware ochrana

Ukládané dokumenty jsou testovány pomocí antiviru (systému na ochranu proti malware).

4.9.6 Plán obnovy (Disaster Recovery)

Dokumentace musí obsahovat stanovení procesů, postupů a opatření pro zajištění obnovy provozu a testování DR plánů.

4.10 Bezpečnostní testy

4.10.1 Systémy, nebo aplikace, které nepublikují služby do veřejné sítě

Systémy, nebo aplikace, které nepublikují služby do veřejné sítě, musí být ve spolupráci s dodavatelem podrobeny internímu bezpečnostnímu testování. Toto testování provádí VZP v součinnosti s dodavatelem.

4.10.2 Systémy, nebo aplikace, které publikují služby do veřejné sítě

a) V případě, že je systém, nebo aplikace bude dostupná z veřejné sítě, musí dodavatel zajistit, aby byl v rámci dodávky proveden nezávislý penetrační test aplikace v rozsahu, který je v souladu s nejlepší praxí.
b) Minimálně jsou provedeny testy v těchto oblastech:

Oblast	**Testy**
Brute Force Prevention	Lack of account lockout, Different login failure message, Insufficient authentication, Weak password recovery, Lack of SSL on login pages, Auto-complete enabled on pass parameters
Credential/Session prediction	Sequential session token, Non-Random session token,
Insufficient Authorization	Forcefully browse to logged in URL, Forcefully browse to high privilege URL, HTTP verb tampering, Insufficient session expiration
Session Fixation	Failure to generate new session ID, Permissive session management
Session Weaknesses	Session token passed in URL, Session cookie not set with secure attribute, Session cookie not set with HTTPOnly, Session cookie not sufficiently random, Site does not force SSL connection, Site uses SSL but references insecure objects, Site supports weak SSL ciphers
Cross-Site Scripting	Reflected cross-site scripting, Persistent cross-site scripting, DOM-based cross-site scripting, Cross-frame scripting, HTML injection, Cross-site request forgery, Clickjacking
Injection Attacks	Format string attack, LDAP injection, OS command injection, SQL injection, Blind SQL injection, SSL injection, XPath injection, HTTP header injection/response splitting, Remote file includes, Local file includes, Potential malicious file uploads
Information Disclosure	Directory indexing, XML External Entity
Information Leakage	Detailed application error messages, Include file source code disclosure, Path traversal, Predictable resource location, Insecure HTTP methods enabled, WebDAV enabled, Default web server files, Testing and diagnostics pages, Internal IP address disclosure, Server-Side Request Forgery (SSRF)

a) Do doby provedení penetračních testů a odstranění nálezů plynoucích z těchto testů nesmí být aplikace veřejně dostupná (technickými prostředky je zajištěno, že je aplikace dostupná pouze subjektu, který provádí testování). Protokol s výsledky testů předkladá dodavatel VZP ČR. Protokol obsahuje metodiku testů, výčet použitých nástrojů při

provedení testů, výčet dílčích testů (dokladuje, které testy byly provedeny) a výsledky testů.

b) Na základě výsledků testů VZP ČR rozhoduje o akceptaci testovaných komponent IS a jejich uvedení do provozu;
c) tento test musí být opakován při každé významné změně systému, nebo aplikace, zejména pokud dochází ke změnám v přístupu k autentizaci a autorizaci systému, nebo aplikace (pokud je systém pod podporou dodavatele, tyto testy provádí dodavatel v rámci režie služby).

Na základě výsledků testů VZP ČR rozhoduje o akceptaci testovaných komponent IS a jejich uvedení do provozu.

5 Logování

Tato kapitola definuje požadavky na logování v oblastech:

a) **Bezpečnosti**:
   a. Základní úroveň logování z pohledu bezpečnosti;
   b. Logování transakcí při zpracování osobních a zvláštních kategorií osobních údajů.
b) **Komunikace a Business logiky**:
   a. Transakční logy.
c) Provozu:
   a. Provozně-aplikační logy.

Pro zalogování událostí do správného logu nebo i do více logů se použije následující logika zařazení události:

Událost související s:	**Oblast logování**
Autentizací	Bezpečnost
Přístupovými oprávněními	Bezpečnost
Privilegované přístupy	Bezpečnost
Operace se soubory	Bezpečnost
Exporty dat	Bezpečnost
Operace s auditními záznamy	Bezpečnost
Operace s osobními daty	Bezpečnost
Stavem aplikace (chyby, výjimky)	Provoz
Stavem infrastruktury	Provoz
Výkonostní aplikace	Provoz
Komunikace s dalšími aplikacemi, použití datových rozhraní	Komunikace

Událost může patřit do více než jednoho logu, tedy bude zalogována do více logů.

5.1 Požadavky

5.1.1 Formát a encoding logu

a) Preferovaný format logu je v případě vývoje aplikace specificky pro VZP ČR JSON (JavaScript Object Notation), **v ostatních případech je formát dán výrobcem** a jeho použití musí být schváleno VZP ČR.
b) Doporučený encoding logu je UTF-8, v ostatních případech je nutné schválení encodingu VZP ČR.

5.1.2 JSON - doporučené pojmenování klíčů a identifikace datové struktury

a) Každý záznam musí obsahovat klíč "`src_type`", který identifikuje datovou strukturu události (přiřazení záznamu příslušné doméně zájmu).
b) Pokud je nutno zaznamenat informace, pro které není vhodné použití žádného z níže uvedených klíčů, pak dodavatel vytváří vlastní klíč:
   i. Klíče jsou pojmenovávány v angličtině.
   ii. Informace o nově vzniklém klíči a jeho účelu je součástí příslušné dokumentace.

5.1.3 Obecně platné zásady pro logování

a) Každý záznam je označen časovým razítkem vytvoření / modifikace záznamu.
b) Logované informace musí odpovídat aktuálnímu stavu systému, interpretace logů musí proveditelná bez dodatečných datových zdrojů. Pokud je logovaná hodnota z číselníku loguje se jak klíč tak i odpovídající hodnotu, které se vždy vztahuji k danému časovému okamžiku.
c) Každá komponenta, která se podílí na zpracování transakcí (včetně volání integračních služeb a rozhraní) bude logovat do lokálního transakčního logu. Do transakčního logu se zaznamenávají minimálně události volání a ukončení služby.

5.1.3.1 Časové razítko

a) Každý záznam obsahuje časové razítko vzniku události.
b) Preferovaný format časového razítka je: "`YYYY-MM-DD hh:mm:ss`", pokud není požadováno jinak, je uvedený čas vždy platný v zóně Europe/Prague. Příklad: "`2019-03-14 11:02:39`".
c) Další možný format časového razítka je ve formátu, ve kterém jej do logu zapisuje operační system, na kterém je aplikace spuštěna (UNIX/Linux: "`Mar 12 13:31:45`", Windows "`15.03.2019 9:31:40`").
d) Ostatní formáty zápisu časového razítka musí být v souladu s ISO 8601 a jejich použití musí být schváleno VZP ČR.

5.1.4 Technické zajištění logování

5.1.4.1 On-Premise

a) Logový soubor musí být lokální, tj. agent nemůže k logu přistupovat pomocí síťového protokolu na sdíleném prostředí. To nevylučuje vzdálené plnění logu. Nepřípustný je log v podobě průběžné databázové tabulky nebo pohledu.
b) Pokud je aplikace nasazena na OS Unix/Linux, pak musí logovat s využitím souborového systému a musí zajistit rotaci logů, nebo využívá mechanismu syslog.
c) Pokud je aplikace nasazena na OS Windows, pak musí logovat s využitím souborového systému a musí zajistit rotaci logů, nebo používá mechanismu Windows Event logu.
d) Musí být zajištěno, aby velikost jedné zprávy nepřekročila 65507 bajtů.

e) Preferovaný mechanismus pro zajištění persistence logů generovaných kontejnery Docker je využití Docker Volumes.

5.1.5 Retence logů

Logy jsou předávány do Centrálního úložiště logů VZP ČR. V ostatních případech (udělena výjimka) musí být zajištěna kapacita pro dostatečně dlouhé uložení logů na příslušných aplikačních serverech, to znamená:

a) všechny logy jsou online uchovány minimálně po dobu 30 dní;
b) logy, které obsahují informace v souladu s požadavky ZoKB, resp. Vyhlášky 82/2018 jsou k dispozici minimálně po dobu 18 měsíců;
c) logy, které obsahují informace o přístupech k osobním údajům nebo k zvláštní kategorii osobních údajů, jsou k dispozici minimálně po dobu 36 měsíců.

5.1.6 Dokumentace

Dodavatelem je předána dokumentace, která obsahuje:

a) výčet auditovaných událostí;
b) vzorky událostí;
c) při použití JSON formátu názvy použitých klíčů vč. jejich popisu;
d) způsob uložení (místo uložení na souborovém systému);
e) zajištění retence a rotace;
f) nastavení přístupových práv.

5.2 Základní úroveň logování z pohledu bezpečnosti

Vlastník kapitoly: OIKB

Pokud jsou záznamy ve formátu JSON, pak každý záznam musí obsahovat následující klíč a kodnotu: `“src_type”: “security”.`

5.2.1 Logování procesu autentizace

Požadavek zaznamenat proce autentizace se týká všech komponent IS VZP ČR, které v jakékoli formě implementují proces autentizace (včetně API).

Auditovaná operace	action	Popis
Přístup do systému nebo aplikace	logon	Jsou zaznamenány všechny oprávněné i neoprávněné pokusy o přístup.
Ukončení práce v systému nebo aplikaci	logout	Je zaznamenáno, kdy byla ukončena práce se systémem - včetně situace, kdy bylo provedeno automatické odhlášení po uplynutí stanovené doby nečinnosti.

5.2.1.1 Příklad logu procesu autentizace u aplikace

Příklad logu procesu autentizace u aplikace, která implementuje vlastní logování a log ukládá do souboru:


```
{ "time_stamp": "2019-03-14 11:02:39", "host_fqdn": "server1.vzp.cz", "host_ip": "172.16.0.1", "src_type": "security", "application": "my_app1", "environment": "prod", "src_class": "VZP_USER", "src_user": "user1", "src_fqdn": "client1.kz.vzp", "src_ip": "172.16.1.1", "src_interface": "UI", "action": "logon", "auth_method": "password", "auth_provider": "ldap", "result": "false", "err_descr": "invalid user" }
```

5.2.2 Činnosti provedené administrátorem

Komponenty IS VZP ČR, které zpracovávají, ukládají, nebo přenáší informace s klasifikací interní a vyšší, musí zaznamenávat:

Auditovaná operace	action	Popis
Činnost administrátora	activity	Jsou zaznamenány činnosti administrátora.

5.2.2.1 Příklad logu činnosti provedené administrátorem

Příklad logu činnosti provedené administrátorem v systému, který implementuje vlastní logování a pro uložení logu využívá syslog:

```
Mar 14 11:02:39 server1 user1: { "time_stamp": "2019-03-14 11:02:39", "origin_fqdn": "server1.vzp.cz", "origin_ip": "172.16.0.1", "src_type": "security", "application": "os_linux", "src_user": "user1", "event_type": "activity", "uid": "root", "gid": "root", "groups": "root", "pid": "17783", "shell": "bash", "action": "tail -f /var/log/messages", "result": "true" }
```

5.2.3 Změny přístupových oprávnění a změny údajů, které slouží k přihlášení

Komponenty IS VZP ČR poskytující služby autentizace nebo autorizace musí zaznamenávat:

Auditovaná operace	Popis
Změny stavu účtu	Přidání, odebrání, zneplatnění, povolení, nebo uzamčením účtu administrátorem (včetně uzamčení účtu po několika neúspěšných pokusech o autentizaci).
Změny rolí přiřazených účtu	Přidání, nebo odebrání role uživatelskému účtu.
Přidání, změna nebo odebrání *definice* role	Jsou zaznamenány všechny aktivity související s přidáním, změnou, nebo odebráním definice role.

5.2.4 Neprovedení činnosti v důsledku nedostatku přístupových oprávnění

Komponenty IS VZP ČR, které zpracovávají, ukládají, nebo přenáší informace s klasifikací interní a vyšší, musí zaznamenávat:

Auditovaná operace	Popis
Neprovedení činnosti	Je zaznamenáno, pokud aktivitu nebylo možno provést v důsledku nedostatečných přístupových oprávnění.

5.2.5 Přístupy k záznamům o činnostech

Komponenty IS VZP ČR, které zpracovávají, ukládají, nebo přenáší informace s klasifikací interní a vyšší, musí zaznamenávat:

Auditovaná operace	Popis
Operace nad auditními záznamy	Komponenty IS VZP ČR musí zaznamenávat pokusy o manipulaci s auditními záznamy a konfigurací auditní služby (v rámci logování přístupu k souborům), včetně zastavení a spuštění mechanismů sloužících pro záznam těchto činností.

5.2.6 Operace se soubory

Pokud soubor obsahuje chráněné informace, pak musí být zaznamenány operace vytvoření, smazání, čtení a zápisu, včetně identifikace uživatele, který operace vykonal.

Auditovaná operace	Popis
Operace se soubory	Jsou zaznamenány operace vytvoření, smazání, čtení a zápisu souboru včetně výsledku operace.
Exporty	Pokud aplikace umožňuje exportovat chráněné informace prostřednictvím UI, pak jsou zaznamenány události exportu dat (uložení dat mimo určenou aplikaci).

5.2.7 Vybrané JSON klíče pro záznam události

Název	Typ	Popis
src_type	VARCHAR2	Identifikuje datovou strukturu události.
time_stamp	DATETIME	Datum a čas zpracování transakce.
origin_fqdn	VARCHAR2	FQDN zařízení, na kterém událost vznikla.
origin_ip	VARCHAR2	IP zařízení, na kterém událost vznikla.
application	VARCHAR2	Jednoznačný identifikátor aplikace, pro kterou záznam vznikl, dle katalogu aplikací (např. application = “crp”).
environment	VARCHAR2	Identifikace prostředí (prod|dev|test).
src_class	VARCHAR2	Typ původce, který inicioval transakci. Může to být například zaměstnanec VZP (VZP_USER), automatická úloha (VZP_JOB), zdravotnické zařízení (ZZ), zdravotní pojišťovna (ZP) atd.
src_user	VARCHAR2	V případě zaměstnance VZP ČR uživatelské jméno, v případě zdravotnického zařízení kód IČZ, v případě zdravotní pojišťovny kód ZP.
dst_user	VARCHAR2	V případě zaměstnance VZP ČR uživatelské jméno, v případě zdravotnického zařízení kód IČZ, v případě zdravotní pojišťovny kód ZP.
src_fqdn	VARCHAR2	Identifikace zařízení (prostředku), ze kterého byla transakce iniciována (FQDN PC nebo serveru, případně reference požadavku IPF).
src_ip	VARCHAR2	Pokud je zařízení (prostředek) PC, nebo server, je uvedena IP adresa prostředku.

dst_fqdn	VARCHAR2	Identifikace zařízení (prostředku), pro který které byla transakce iniciována (FQDN PC nebo serveru, případně reference požadavku IPF).
dst_ip	VARCHAR2	Pokud je zařízení (prostředek) PC, nebo server, je uvedena IP adresa prostředku.
detail	VARCHAR2	Pole pro doplňující komentář nebo jiné informace.
src_interface	VARCHAR2	Identifikace volajícího rozhraní (např. UI, IPF, CRON).
action	VARCHAR2	Typ události / akce.
result	BOOLEAN	Výsledek operace (true == provedeno|false == selhalo).
error_descr	VARCHAR2	Upřesnění chyby v případě selhání.

5.3 Logování transakcí při zpracování osobních a zvláštní kategorie osobních údajů

Vlastník kapitoly: OKIB

Pokud tranakce provádí operace, které lze vztáhnout k určenému nebo určitelnému subjektu údajů, jsou vždy zaznamenávány auditní informace, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní nebo zvláštní kategorie osobních údajů, zaznamenány nebo jinak zpracovány. Vždy je rovněž zaznamenán výčet primárních aktiv typu informace, které se transakce účastní.

Nad rámec transakcí zpracování osobních údajů a zvláštní kategorie osobních údajů údajů jsou zaznamenávány náhledy a změny zdravotní pojišťovny vzhledem k přímé vazbě na zpracování OÚ a pro možné prošetřování zejména neoprávněné přeregistrace ke zdravotní pojišťovně, případně provedené změny bez vědomí a souhlasu pojištěnce.

Záznamy transakcí při zpracování osobních údajů ve formátu JSON musí obsahovat identifikaci datové struktury `“src_type”: “data_access”` a identifikaci události `“action”:` s výčtovou hodnotou `“data_create” OR “ data_read” OR “data_update” OR “data_delete”` (CRUD).

a) Logování zajistí komponenta, která je původcem transakce.
b) Vždy je zajištěna jednoznačná identifikace iniciátora transakce a to i při zřetězení transakce.
c) Ze zaznamenané tranakce musí být zjevné, zda je událost vyvolána interakcí uživatele s UI, nebo zda se jedná o automatizovaný proces.
d) Pro zaznamenání, z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, je využit číselník důvodů.

5.3.1 Vybrané JSON klíče pro záznam události

Název	**Typ**	**Popis**
detail	VARCHAR2	Z jakého důvodu byly osobní údaje, nebo zvláštní kategorie osobních údajů zaznamenány, nebo jinak zpracovány.
subject_id	VARCHAR2[]	Identifikátor subjektu, nebo subjektů tak, jak jej využívá aplikace.
subject_attr	VARCHAR2[]	Výčet konkrétních informačních aktiv, které se účastní transakce.
file_name	VARCHAR2	Jméno souboru, pokud se účastní transakce.

5.3.2 Příklad logu činnosti nahlížení

Příklad logu nahlížení údaje subjektu z UI aplikace:


```
{ "time_stamp": "2019-03-14 11:02:39", "origin_fqdn": "server1.vzp.cz", "origin_ip": "172.16.0.1",
"src_type": "data_access", "application": "my_app1", "environment": "prod", "src_class": "VZP_USER",
"src_user": "user1", "src_fqdn": "client1.kz.vzp", "src_ip": "172.16.1.1", "src_interface": "UI",
"action": "data_read", "result": "true", "detail": "kontrola údajů klienta, žádost klienta", "subject_id
": "54a2ca2e4f47e95870cdcd9b216588d7", "subject_attr": { "pojistenec": [ "cisloPojistence", "jmeno",
"prijmeni", "datumNarozeni" ], "aktualniAdresa": [ "ulice", "obec", "psc", "stat" ] } }
```


5.3.3 Příklad logu činnosti změna

Příklad logu změny zdravotní pojišťovny z UI aplikace:


```
{ "time_stamp": "2019-03-14 11:02:39", "origin_fqdn": "server1.vzp.cz", "origin_ip": "172.16.0.1",
"src_type": "data_access", "application": "my_app1", "environment": "prod", "src_class": "VZP_USER",
"src_user": "user1", "src_fqdn": "client1.kz.vzp", "src _ip": "172.16.1.1", "src_interface": "UI",
"action": "data_write", "result": "true", "reason": "přeregistrace klienta k jiné ZP", "subject_id ":
"54a2ca2e4f47e95870cdcd9b216588d7", "subject_attr": { "zdravotniPojistovna": [ "kod", "nazev" ] } }
```


5.4 Základní požadavky na logování komunikace a business logiky- Transakční log[7]

Vlastník kapitoly: OAVRZ

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. Výčet zaznamenávaných událostí odpovídající business logice je povinnou součástí návrhu a dokumentace systému.

5.4.1 Informační obsah události zaznamenávané v transakčním logu

Pokud jsou záznamy ve formátu JSON, pak každý záznam musí obsahovat následující klíč a kodnotu: `“src_type”: “transaction”.`

Auditovaná událost /operace	**Popis**
Volání rozhraní aplikační komponenty	Komponenty IS VZP ČR musí zaznamenávat volání svého aplikačního rozhraní.
Zápis a čtení zpráv do/z fronty zpráv	Komponenty IS VZP ČR musí zaznamenávat předávání dat pomocí front (mesagingu)
Synchronizace dat pomocí rozhraní pro dávkové zpracování	Komponenty IS VZP ČR musí zaznamenávat výměnu dat pomocí dávkového zpracování dat (ETL, file sync apod.)
Směrování zpráv v rámci integrační platformy	Komponenty IS VZP ČR musí zaznamenávat případné podmíněné směrování zpráv, případně volání. Relevantní zejména pro integrační vrstvu (ESB, BPEL engine apod.)

[7] 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.

Transformace zpráv	Komponenty IS VZP ČR musí zaznamenávat transformace zprávy na jiný formát. Relevantní zejména pro integrační a proxy komponenty.

5.4.2 Vybrané JSON klíče pro záznam události

Název	Typ	Popis
src_type	VARCHAR2	Identifikuje typ události.
time_stamp	DATETIME	Datum a čas zápisu záznamu
origin_fqdn	VARCHAR2	FQDN zařízení, na kterém událost vznikla.
origin_ip	VARCHAR2	IP zařízení, na kterém událost vznikla.
application	VARCHAR2	Jednoznačný identifikátor aplikace, pro kterou záznam vznikl, dle katalogu aplikací (např. application = “crp”).
environment	VARCHAR2	Identifikace prostředí (prod|dev|test).
app_interface	VARCHAR2	Identifikace použitého rozhraní, zahrnuje typ rozhraní
service_id	VARCHAR2	Identifikátor použité služby – tím je myšleno ID(uri) rozhraní / ID fronty zpráv apod.
instance_id	VARCHAR2	Jednoznačný identifikátor instance dané transakce/služby přidělovaný zapisující službou / aplikací
com_partner	VARCHAR2	Jednoznačný identifikátor protistrany komunikace podle katalogu aplikací (pokud je znám)
transaction_id	VARCHAR2	Identifikátor primární business transakce – události předávaný přes všechna volání podřízených služeb
partner_id[8]	VARCHAR2	Technologický identifikátor partnera, kterého se volání

[8] ID_PARTNER slouží k logování pro GDPR, 101/2000 Sb. a ZoKB jako zdroj informaci o žádajícím subjektu

		služby týká, předávaný přes všechna volání podřízených služeb.
src_user	VARCHAR2	Identifikace uživatele, který spustil primární službu. Předávaný přes všechna volání podřízených služeb.
result	BOOLEAN	Výsledek operace (true == provedeno|false == selhalo).
result_code	VARCHAR2	Výstupní stav dané instance transakce/služby kód stavu

5.4.3 Příklad transakčního logu

Příklad záznamu volání aplikace přes webové rozhraní

```
{ "time_stamp": "2019-03-14 11:02:39", "origin_fqdn": "server1.vzp.cz", "origin_ip": "172.16.0.1", "src_type": "transaction", "application": "my_app1", "environment": "prod", "app_interface": "SOAP", "service_id": "soa-infra/services/ZakladniRegistry/AiscCtiAifo/client", "instance_id": "a4567gdsfx4460", "com_partner": "B2B_proxy", "transaction_id": "a02546456fd464d45s46z1x", "partner_id": " client1.kz.vzp ", "src_user": " user1 ", "result": "true", "result_code": "200 OK" }
```

5.5 Provozní log

5.5.1 Základní požadavky na provozní logování – Provozní log

5.5.2 Formát logovacího souboru provozního logu

Formát provozních logů je specifický z důvodu specifických požadavků na rychlé a automatizované zpracování:

- Formát souboru je 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.
- 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 provozního logu:

Název	**Popis**
time_stamp	Datum a čas zápisu záznamu ve formátu dle kapitoly 5.1.3.1 Časové razítko

při zpracování. Vlastní logování zpracovávaných osobních údajů (subjektů), kterých se daná transakce týká zajistí komponenta, která je původcem dané transakce

severity	Hodnocení závažnosti události viz níže.
Proces	Proces, ke kterému se vztahuje událost, nepovinné
object	objekt, který je zdrojem zprávy (např. program, název certifikátu, apod.), nepovinné
text	text zprávy, obsahující popis události a případné chyby

5.5.2.1 Závažnost provozní události podle výsledku operace

Závažnost	**Popis**
Critical	Fatální chyba, např. nemožnost spustit operaci, kdy je nutný zásah v co nejkratší době.
Major	Výsledek operace je selhání operace, např. neúspěchu posledního z pokusů o přenos, kdy je nutný zásah, např. manuální zpracování.
Minor	Neúspěch běhu operace, operace bude opakována, nebo nastala dílčí chyba, která nemusí znamenat neúspěch celé akce. Je žádoucí kontrola průběhu.
Warning	Zjištění problémů u operace s úspěšným výsledkem nebo jiná upozornění, která vyžadují příležitostné prověření.
Normal	Úspěšné dokončení operace.

6 Provozní standardy

6.1 Monitoring

Vlastník kapitoly: OTP OCD

6.1.1 Rozsah monitoringu a používané nástroje

Rozsah monitoringu a používané monitorovací nástroje jsou popsány v dokumentu Stav IS VZP.

6.1.2 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
- **Business Process Monitor (BPM)** – aktivní 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.

6.1.3 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 v kapitole 5.5 Provozní log.

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.

6.1.4 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.

6.1.5 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 vytvořen podle kapitoly 5.5 Provozní log

6.2 Zálohování a archivace

Vlastník aplikace: OTP OSSU

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

6.2.1 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.

6.2.2 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

6.3 Definice provozních parametrů služby/aplikace (SLA)

Vlastník kapitoly: OTP OSAD

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
1. Po 18:00 - 24:00 HW údržba
2. Út 18:00 - 24:00 SW údržba
3. St 18:00 - 24:00 HW údržba
4. Čt 18:00 - 24:00 SW údržba

Podpora Helpdesk - standardní doba Helpdesku pro uživatele a řešitele -
Režim podpory Helpdesku
5. Po – Čt 07:00 - 17:00
6. 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.

6.4 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

6.5 Vazba na ITIL procesy

Vlastník kapitoly: OKP

Aplikace musí být zařazena ve VZP do standardních ITIL procesů.

6.5.1 Definování veškerých eskalačních procedur u aplikace - správa HelpDesku/ServiceDesku

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

6.5.2 Zavedení aplikace do incident managementu

Aplikace musí být zavedena do procesu Incident Managementu.

6.5.3 Zavedení aplikace pod standardní řízení změn - change management

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

- Požadavek a zadání změny
- Schvalovací proces změny
- Realizace změny a předání úpravy aplikačního softwarového vybavení (dále zkratkou ASW) podle pravidel release managementu (uvedeno v následující kapitole)
- Nasazení změny ASW a akceptace v rámci procesu test managementu
- Podle objemu a závažnosti zakázky je může být celý proces projektově řízen.

6.5.4 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.

7 Seznam příloh

Příloha 1: Vzor_Predavaci_tabulky_PP (produkční prostředí)
Příloha 2: Vzor_Predavaci_tabulky_TP (testovací prostředí)
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

8 Výjimky ze standardu

8.1 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