Nefunkční požadavky

Obsah

[Nefunkční požadavky 1](#_Toc488391484)

[1 Architektura a technologie 2](#_Toc488391485)

[1.1 Technická infrastruktura 4](#_Toc488391486)

[1.1.1 Vymezení odpovědností Zadavatele a Dodavatele 4](#_Toc488391487)

[1.2 Prostředí systému RPIS 5](#_Toc488391488)

[1.3 Požadavky na dostupnost systému RPIS a jeho provozní doba 6](#_Toc488391489)

[1.4 Servisní odstávky RPIS 6](#_Toc488391490)

[1.5 Požadavky na realizaci díla – přístup do NDC 6](#_Toc488391491)

[1.6 Standardy a stavební bloky SPCSS 7](#_Toc488391492)

[1.6.1 Specifikace NDC 7](#_Toc488391493)

[1.6.2 Bezpečné propojení a připojení do Internetu 7](#_Toc488391494)

[1.6.3 Poskytování výpočetního výkonu 8](#_Toc488391495)

[1.6.4 Poskytování diskového prostoru 9](#_Toc488391496)

[1.6.5 Správa operačních systémů 10](#_Toc488391497)

[1.6.6 Správa databází 10](#_Toc488391498)

[1.6.7 Zálohování a archivace dat 11](#_Toc488391499)

[1.6.7.1 Popis zálohování a archivace Zadavatele 11](#_Toc488391500)

[1.6.7.2 Požadavky na zálohování, archivaci a obnovu RPIS 11](#_Toc488391501)

[1.6.7.2.1 Archivace v RPIS 11](#_Toc488391502)

[1.6.7.2.2 Zálohování v RPIS 12](#_Toc488391503)

[1.6.7.2.3 Obnovení systému RPIS 12](#_Toc488391504)

[1.6.8 SW licence a subskripce 13](#_Toc488391505)

[2 Role, výkonnost, kapacita, škálovatelnost RPIS 13](#_Toc488391506)

[2.1 Role v RPIS 13](#_Toc488391507)

[2.2 Výkonnost a kapacita RPIS 14](#_Toc488391508)

[3 Požadavky na bezpečnost 14](#_Toc488391509)

[3.1 Obecné požadavky na bezpečnost 14](#_Toc488391510)

[3.2 Návrh řešení bezpečnosti 15](#_Toc488391511)

[4 Logování, provozní a bezpečnostní monitoring 15](#_Toc488391512)

[4.1 Popis provozního monitoringu Zadavatele 15](#_Toc488391513)

[4.2 Požadavky na provozní monitoring RPIS 16](#_Toc488391514)

[4.3 Popis bezpečnostního monitoringu (CKB a SOC) Zadavatele 16](#_Toc488391515)

[4.4 Požadavky na bezpečnostní monitoring RPIS 16](#_Toc488391516)

[5 Autentizace a autorizace 16](#_Toc488391526)

[6 Důvěrnost a integrita 17](#_Toc488391527)

[7 Auditovatelnost a nepopiratelnost 18](#_Toc488391528)

[8 Rozhraní systému 20](#_Toc488391529)

[9 Podpora, provoz a údržba, klasifikace chyb 21](#_Toc488391530)

[9.1 Definice provozní podpory RPIS 21](#_Toc488391531)

[9.2 Podpora první úrovně (L1) 21](#_Toc488391532)

[9.3 Podpora druhé úrovně (L2) 21](#_Toc488391533)

[9.4 Podpora třetí úrovně (L3) 22](#_Toc488391534)

[9.5 SLA podpory první úrovně (L1) a Service Desk 22](#_Toc488391535)

[9.5.1 Provozní doba 22](#_Toc488391536)

[9.5.2 Reakční doba 22](#_Toc488391537)

[9.6 SLA podpory druhé úrovně (L2) 23](#_Toc488391538)

[9.6.1 Provozní doba 23](#_Toc488391539)

[9.6.2 Reakční doba 23](#_Toc488391540)

[9.7 SLA podpory třetí úrovně (L3) 23](#_Toc488391541)

[9.7.1 Provozní doba 23](#_Toc488391542)

[9.7.2 Reakční doba 23](#_Toc488391543)

[9.7.3 Doba opravy 23](#_Toc488391544)

[9.8 Klasifikace chyb 23](#_Toc488391545)

[10 Rozvojové požadavky na RPIS – Služby rozvoje 24](#_Toc488391546)

[10.1 Objednávání Služeb rozvoje 24](#_Toc488391547)

[10.2 Akceptace Služeb rozvoje 25](#_Toc488391548)

[11 Školení 25](#_Toc488391549)

[11.1 Školení metodických pracovníků OSS 25](#_Toc488391550)

[11.2 Školení administrátorů první a druhé úrovně podpory 25](#_Toc488391551)

[11.2.1 Školení administrátorů první úrovně podpory 25](#_Toc488391552)

[11.2.2 Školení administrátorů druhé úrovně podpory 25](#_Toc488391553)

[12 Další požadavky 26](#_Toc488391554)

[12.1 Migrace 26](#_Toc488391555)

# Architektura a technologie

Nový Resortní personální informační systém (dále jen RPIS) bude postaven na vícevrstvé architektuře umožňující v případě potřeby provozování jednotlivých vrstev v interním (privátním) cloudu, včetně škálovatelnosti výkonu jednotlivých vrstev. Základní dělení vrstev je zobrazeno na následujícím schématu.



Architektonické schéma IS RPIS

Řešení klientské části aplikace může být pro jednotlivé skupiny uživatelů postaveno na tenkém klientu nebo může být instalováno na uživatelské stanici.

Pro žádnou vrstvu architektury RPIS nejsou stanovena omezení na konkrétní hardware, operační systém, databázový systém ani webový prohlížeč. Použité technologie musí umožňovat provozování ve virtualizovaném prostředí. RPIS musí podporovat připojení klientů z prostředí LAN, WAN i VPN kanálem z internetu.

RPIS musí umožnit efektivní a bezpečnou koexistenci několika organizací, které se budou významně lišit velikostí, typy pracovněprávních vztahů resp. služebních poměrů, geografickým rozložením pracovišť apod. Je vyžadováno, aby Dodavatel navrhl a popsal řešení, které bude těmto požadavkům vyhovovat, a to do dokumentu příloze č. 10 Požadavky na technický návrh řešení.

## Technická infrastruktura

* + 1. Vymezení odpovědností Zadavatele a Dodavatele

V souladu se strategií ICT resortu Ministerstva financí bude RPIS vybudován a provozován v prostředí Národního datového centra (dále jen „NDC“) resortního dodavatele služeb infrastruktury a provozu Státní pokladny Centra sdílených služeb, s. p. (dále jen „SPCSS“). Cílem této strategie je dosažení maximální efektivity sdílených služeb IT infrastruktury v resortu Ministerstva financí v souladu se strategií rozvoje eGovernmentu ČR.

Dodávku, implementaci a provoz síťové, HW a SW infrastruktury a související provozní služby (zálohování, monitoring) zajistí SPCSS podle návrhu Dodavatele.

SPCSS bude poskytovat infrastrukturu a související služby formou provozních služeb na svých sdílených platformách, včetně přípravy těchto služeb pro implementaci RPIS. Konkrétně jde o oblasti:

* Služby datového centra
* Bezpečné propojení a připojení do Internetu (síťové služby)
* Poskytování výpočetního výkonu (včetně virtualizace)
* Poskytování diskového prostoru
* Správa operačních systémů
* Správa databází (pouze provozní služby v rámci Servisních služeb, dodávka, SW licence včetně maintenance a implementace v odpovědnosti Dodavatele)
* Zálohování a archivace dat
* CKB, SOC a bezpečnostní monitoring
* Provozní monitoring
* Service Desk

Návrh kompletní technické infrastruktury RPIS je odpovědností Dodavatele. Dodavatel navrhne a popíše technickou infrastrukturu včetně jejího kapacitního návrhu na základě požadavků uvedených v této příloze. V návrhu technické infrastruktury Dodavatel použije standardy a stavební bloky SPCSS, uvedené v kapitole 1.6 „Standardy a stavební bloky SPCSS“ této přílohy a popíše ji podle požadavků ve smyslu této ZD v příloze č. 10 Požadavky na technický návrh řešení.

V rámci realizace Díla a poskytování Servisních služeb a rozvoje bude Dodavatel spolupracovat se SPCSS v rámci součinností souvisejících s implementací, provozem technické infrastruktury a souvisejících provozních služeb SPCSS. Detailní rozdělení odpovědností mezi Dodavatele a SPCSS a rozsah součinností při realizaci Díla definuje Dodavatel v dokumentu „Požadavky na technický návrh řešení.“

Rozdělení odpovědností Dodavatele a Zadavatele v implementaci i provozu vychází z výše uvedeného vymezení dodávky SPCSS.

## Prostředí systému RPIS

Je požadována implementace minimálně těchto prostředí s tím, že některá z nich mohou být sdílená a optimalizovaná pro svůj účel použití:

* Produkční
* Školicí/Pre-produkční
* Testovací

Dodavatel může v návrhu použít více oddělených prostředí, pokud je takové použití v souladu s plněním požadavků na systém v rozsahu ZD.

Pro jiná než produkční a pre-produkční prostředí Dodavatel navrhne a zajistí způsob a postupy pro anonymizaci dat (například při aktualizacích systémů nebo opětovném plnění dat).

Plnění SLA dostupnosti systému uvedených v kapitole 1.3 lze zajistit redundancí HW i SW komponent na všech vrstvách produkčního prostředí.

Pre-produkční prostředí musí obsahovat stejné mechanismy redundance HW a SW produkčního prostředí, jeho výkon a datové kapacity musí odpovídat potřebám testování v rámci Servisních služeb a Služeb rozvoje. Zátěžové testy budou provedeny na Produkčním prostředí před spuštěním ostrého provozu, nebo na Pre-produkčním prostředí s dočasně navýšenými HW zdroji.

Před nasazením nové verze sw na předprodukční resp. produkční prostředí je požadována aktualizace dokumentace a zdrojové kódy.

## Požadavky na dostupnost systému RPIS a jeho provozní doba

Systém bude dostupný v režimu 7x24 s povolenými plánovanými servisními odstávkami uvedenými v kapitole 1.4.

V době mimo plánované servisní odstávky činí požadovaná dostupnost:

99,5 % na roční bázi (tj. maximální celková přípustná doba nedostupnosti za kalendářní rok činí 44 hodin)

98,9 % na měsíční bázi (tj. maximální celková přípustná nedostupnosti za kalendářní měsíc činí 8 hodin)

Požadovaná provozní doba, jako období, kdy musí být zajištěny všechny služby související s provozem systému a nesmí být plánovány servisní odstávky, je 5x10 hodin, tedy v pracovní dny mezi 8. a 18. hodinou.

## Servisní odstávky RPIS

Servisní odstávky jsou přípustné v maximálním rozsahu 96 hodin ročně. Jednotlivá servisní odstávka nesmí přesáhnout 24 hodin.

Servisní odstávky musí být realizovány mimo nadefinovanou provozní dobu systému a mimo období požadované zvýšené dostupnosti. Zvýšená dostupnost jsou poslední dva pracovní dny v měsíci a prvních 5 pracovních dnů nového měsíce. Servisní odstávky by měly být přednostně plánovány na víkendy a svátky.

Typy servisních odstávek

* plánované servisní odstávky
* mimořádné servisní odstávky

Plán servisních odstávek a období zvýšené dostupnosti bude sestaven vždy na celý kalendářní rok a včas předložen ke schválení Zadavatelem.

Mimořádné servisní odstávky, kromě odstávek pro řešení havarijních stavů, musí být plánovány minimálně jeden týden předem a oznámeny uživatelům formou publikování informací v RPIS.

## Požadavky na realizaci díla – přístup do NDC

Ke všem implementovaným prostředím bude Dodavateli poskytnut vzdálený přístup pomocí VPN, a to buď propojením sítí přes VPN, nebo jako přístup jednotlivých rolí Dodavatele s využitím PC klientů a dvoufaktorové autentizace. Podporovaná technologie je Cisco VPN (Cisco Anyconnect). Konkrétní nastavení propojení sítí bude po dohodě s Dodavatelem.

Umístění pracovníků Dodavatele v prostorách SPCSS, kromě pracovníků podpory Dodavatele v rámci post implementační podpory nebo školení pracovníků SPCSS, se nepředpokládá.

## Standardy a stavební bloky SPCSS

* + 1. Specifikace NDC

Národní datové centrum (NDC) SPCSS se nachází na adrese Na Vápence 915/14, Žižkov, 130 00 Praha 3. Hlavní parametry NDC jsou prostředí dle normy TIER III ANSI/TIA – 942/The Uptime Institute a možnost provádění servisních prací za plného provozu datového centra SPCSS bez dopadu na zákazníky a jejich zařízení. NDC nabízí redundanci všech kritických systémů a fyzickou bezpečnost, která je zajišťována nepřetržitou fyzickou ostrahou a evidencí vstupu a monitoringem oprávněných osob uvnitř datového centra.

Druhé datové centrum NDC Zeleneč je ve výstavbě a bude v provozu od roku 2019. NDC Zeleneč bude připojeno dostatečnou kapacitou pro zajištění LAN a SAN konektivity mezi lokalitami. Síťová infrastruktura propojení mezi datovými centry umožní bezproblémové použití synchronní replikace dat na úrovni diskových polí.

V případě požadavku podpory Disaster Recovery (obnova infrastruktury systému po havárii, dále jen „DR“) požadované pro některé kritické komponenty řešení, může SPCSS zajistit umístění DR systémů v oddělené místnosti s plně nezávislou podporou na všech úrovních (napájení, chlazení, síťové připojení) a výhledově možnost přesunu DR systémů do druhé lokality. Využití druhé lokality je možné pro všechny části řešení podle návrhu Dodavatele.

* + 1. Bezpečné propojení a připojení do Internetu

SPCSS provozuje síťovou infrastrukturu včetně telekomunikačních linek a aktivních síťových bezpečnostních prvků, zahrnující redundantní připojení do internetu a NIXu s vlastním AS, propojení do CMS a KIVS, propojení do resortních sítí (GOVBONE), ochranu proti DoS a DDoS útokům, ochranu proti síťovým útokům (IPS, IDS), SSL terminátory (SSL akcelerátory, SSL off-loadery), síťové firewally, webový aplikační firewall (WAF), load balancery.

Součástí síťové infrastruktury SPCSS jsou rovněž standardní síťové služby NTP, DNS, e-mail a VPN (vzdálený přístup). Síťová infrastruktura SPCSS je plně integrována do provozního a bezpečnostního monitoringu SPCSS. Část návrhové, implementační a provozní dokumentace síťové infrastruktury SPCSS je chráněna v režimu utajovaných informací stupně Vyhrazené dle Zákona o ochraně utajovaných informací.

Bezpečnostní standardy SPCSS obecně nevyžadují šifrování vnitřních komunikací, šifrovaná komunikace na vnitřních sítích se používá ve vybraných případech podle bezpečnostních požadavků příslušného IS.

Primární úroveň antivirové ochrany na úrovni serverů je zajišťována Zadavatelem a je součástí služeb.

Primární úroveň antivirové ochrany na klientských stanicích je zajišťována IT příslušné OSS.

* + 1. Poskytování výpočetního výkonu

SPCSS provozuje v rámci svých služeb privátní cloud formou IaaS. Standardem je platforma x86, 64bit. Privátní cloud je rozdělen do dvou datových center (DC1, DC2), v každém datovém centru je dále rozdělen do dvou virtualizačních domén umístěných na oddělených HW platformách. V oblasti virtualizace jsou podporovány technologie KVM, VMware a MS Hyper-V. SW licence virtualizace jsou součástí služby SPCSS. Součástí služby jsou i aktualizace verzí virtualizačního SW.

K dispozici jsou tři plány alokace vCPU a vRAM do výpočetních bloků. Plán A pro standardní aplikace optimálně zohledňující poměr vCPU a vRAM a dále plán B pro procesorově náročnější aplikace a plán C pro paměťově náročné aplikace. Níže uvedená tabulka blíže specifikuje konfiguraci základních výpočetních bloků pro jednotlivé plány:

|  |  |  |  |
| --- | --- | --- | --- |
| **Základní výpočetní blok** | **Procesor** | **Počet vCPU (core)** | **vRAM (GB)** |
| Plán A | E5-2630 v3 (Haswell) 3.2GHz  | 1 | 4 |
| Plán B | E5-2698 v3 (Haswell) 3.6GHz  | 1 | 2 |
| Plán C | E5-2698 v3 (Haswell) 3.6GHz | 1 | 8 |

Každý plán je daná kombinace vCPU a vRAM. Zdroje požadované pro virtuální instanci jsou pak násobkem základního výpočetního bloku. V případě, že požadovaný poměr počtu vCPU a GB vRAM nevyhovuje jednomu z uvedených plánů (např. poměr 1:3), je nutno použít nejbližší vhodný plán a jeho násobek pokrývající jak potřeby vCPU, tak vRAM (v uvedeném příkladu to mohou být 2 bloky v plánu B nebo 1 blok v plánu A).

Všechny plány využívají stejnou síťovou infrastrukturu a mají shodný síťový profil. Virtualizované bloky výpočetního výkonu je možno použít ve všech bezpečnostních zónách včetně DMZ.

Pro potřeby návrhu a zajištění požadované dostupnosti a geografické redundance lze pro každou virtuální instanci možné specifikovat následující parametry:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Hodnoty** | **Vysvětlení** |
| Lokalita | DC1/DC2  | Umístění na virtualizační platformě v datovém centru DC1 nebo DC2. |
| Redundance | Ne/Doména/DC | **Ne – dostupnost 99,5 %** ročně - nemá alokovanou pasivní zálohu, nebo má pasivní zálohu v rámci jedné virtualizační domény (není garantováno umístění na jiném HW) **Doména – dostupnost 99,982 %** ročně - má alokovanou pasivní zálohu v jiné virtualizační doméně (garantováno umístění na jiný HW) ve stejném datovém centru**DC – dostupnost 99,99 %** ročně - má alokovanou pasivní zálohu v jiném datovém centru (geografická redundance)Poznámka: alokovaný prostor pro pasivní zálohu umožňuje migraci virtuální instance v případě výpadku HW na jiný server virtualizační farmy ve stejné nebo jiné lokalitě prostředky virtualizační platformy  |

V oblasti operačních systémů jsou podporovány operační systémy MS Windows Datacenter 2012 a novější a Linux CentOS (Red Hat Enterpise Linux) verze 7.0 a novější (tedy verze Linux kernelu 3.10 a vyšší), SUSE Linux Enterprise Server 12 SP2 a novější. SW licence OS jsou součástí služby SPCSS.

* + 1. Poskytování diskového prostoru

SPCSS poskytuje následující služby diskových polí:

|  |  |  |
| --- | --- | --- |
| **Kód jednotky** | **Název jednotky (nemusí se shodovat se skutečným účelem)** | **Popis** |
| STOR1 | Produktivní pole | Rychlá high-end storage. Pro soubory o velikosti 500 GB pole dosahuje min. **15 000 IOPS pro zápis a 35 000 IOPS** pro čtení a a propustnost **2000 MB/s.** STOR1 podporuje využití flash disků, včetně dedikování určité flash-only diskové kapacity. |
| STOR2 | Sekundární pole | Non high-end storage. **Nejsou poskytovány garance propustnosti nebo IOPS**. Průměrné hodnoty jsou až 10 000 IOPS na 250 GB pro zápis a propustnost 650 MB/s. Doba doručení změn je do 10 % 5 dní, nad tento limit 40 pracovních dní. |
| BACK | Backup pole | Uložená data s přenosem po Ethernetu, rychlost obnovy 100 GB/h a vyšší. Pro soubory o velikosti 250 GB pole dosahuje 10 000 IOPS pro zápis |
| BACK2 | Backup/Restore normal | Uložená data s přenosem výhradně po ethernetu, rychlost 11 GB/h |
| BACK3 | Longterm Backup/Restore | Uložená data s retencí 1 rok a delší pro dlouhodobé archivace. |

Pro potřeby návrhu a zajištění požadované dostupnosti a geografické redundance lze pro každý diskový prostor na STOR1 nebo STOR2 specifikovat následující parametry:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Hodnoty** | **Vysvětlení** |
| Lokalita | DC1/DC2 | Umístění v datovém centru DC1 nebo DC2 |
| Redundance | Lokální/DC  | **Lokální – dostupnost 99,982 %** ročně - asynchronní záložní kopie dat na jiném diskovém poli ve stejném DC**DC – dostupnost 99,99 %** ročně- asynchronní záložní kopie dat na diskovém poli v jiném datovém centru (geografická redundance)  |

Replikace dat na úrovni diskových úložišť je k dispozici, v současnosti je využívána synchronní replikace mezi poli. Propustnost replikační linky lze uvažovat 8 Gbit.

* + 1. Správa operačních systémů

Instalaci, konfiguraci a správu operačních systémů na úrovni fyzických i virtuálních serverů provádí SPCSS. Administrátorské účty OS jsou v rukou SPCSS. Dodavatel používá pro implementaci a podporu provozu databází a aplikací uživatelské účty, využití administrátorských účtů je možné pouze se součinností SPCSS nebo bezpečným mechanismem schváleným SPCSS (např. sudo s nastavením specifických povolených příkazů). Dodavatel musí navrhnout implementaci aplikací tak, aby eliminoval, respektive snížil na minimální nutnou úroveň nutnost použití administrátorských účtů při provozní podpoře aplikací.

SW licence OS a virtualizace jsou součástí služby SPCSS. Součástí správy operačních systémů je provádění aktualizací verzí OS a virtualizačních platforem. Aktualizace aplikačního SW bude plánována ve spolupráci s Dodavatelem.

Součástí služby SPCSS není implementace a správa aplikačních komponent operačních systémů, respektive aplikačního SW přibaleného k základnímu OS, jako jsou například web servery, aplikační servery, middleware, databáze nebo adresářové služby pro účely správy aplikačních uživatelů. Dodavatel může takové komponenty využít a využít i jejich licencí v rámci licencí OS pořízených SPCSS, nicméně je odpovědný za jejich implementaci a podporu. Seznam těchto aplikačních komponent vyplní v příloze č. 10 Požadavky na technický návrh řešení.

* + 1. Správa databází

Instalaci a prvotní konfiguraci databází provede Dodavatel. Správu databází bude provádět SPCSS. Administrátorské účty databází a účty vlastníků schémat jsou v rukou SPCSS. Dodavatel může použít pro implementaci a podporu aplikací uživatelské účty, využití administrátorských účtů a účtů vlastníků schémat je možné pouze se součinností SPCSS. Dodavatel musí navrhnout implementaci databází a aplikací tak, aby eliminoval, resp. snížil na minimální nutnou úroveň nutnost použití administrátorských účtů a účtů vlastníků schémat při provozní podpoře aplikací.

Součástí správy databází je provedení aktualizací verzí DB. Aktualizace SW bude plánována ve spolupráci s Dodavatelem.

SW licence databází není součástí služby SPCSS, licence, maintenance a/nebo subskripce databází potřebných pro implementaci a provoz RPIS jsou součástí dodávky Dodavatele a musí být uvedeny v seznamu SW licencí v příloze č. 10 Požadavky na technický návrh řešení.

* + 1. Zálohování a archivace dat

####  Popis zálohování a archivace Zadavatele

Služba je poskytována v rozsahu uvedeném v backup plánech, jejichž návrh je dodávkou Dodavatele a je popsán v příloze č. 10 Požadavky na technický návrh řešení. Backup plán v souladu s nefunkčními požadavky musí obsahovat minimálně následující údaje:

1. co se zálohuje (například disk c://filesystem/home, všechny lokální filesystémy)
2. co se nemá zálohovat (například nezálohovat adresář c:\tmp, nezálohovat adresáře s daty v rámci zálohy filesystemu)
3. kdy se zálohuje (čas spuštění zálohy a frekvence opakování)
4. typ zálohy (plná, přírůstková, differential a podobně)
5. retence dat (jak dlouho budou data uložena, například dva měsíce)

Služba je poskytována pomocí software Tivoli Spectrum Protect. SW licence zálohovacího systému jsou součástí služby. Součástí služby jsou i aktualizace verzí zálohovacího SW. Aktualizace SW bude plánována ve spolupráci s Dodavatelem a Zadavatelem.

Mezi další požadavky může být zahrnuto i držení dat ve více kopiích, specifikace RTO (jak rychle musí být data obnovena), specifikace RPO (maximální povolená doba ztráty dat), časové omezení backup okna (záloha musí doběhnout do tří hodin od startu) a podobně.

Pásky mohou být na vyžádání vyjmuty a uloženy do trezorů, umístněných v samostatných trezorových místnostech v oddělené režimové zóně. TSM servery a jejich disková pole jsou umístněny v oddělených režimových zónách od páskových knihoven. Každá z uvedených zón je současně samostatným požárním úsekem vybaveným SHZ a EPS s odpovídajícím zajištěním fyzické bezpečnosti.

####  Požadavky na zálohování, archivaci a obnovu RPIS

##### Archivace v RPIS

Data v plné šíři záznamů musí být dostupná on-line pro všechny aktivní pracovně právní vztahy (PPV) a pro ukončené PPV po nadefinovanou dobu od data ukončení (např. 10 let). Poté mohou být data archivována a zredukována.

V rámci plné šíře záznamů musí být on-line dostupná data potřebná pro výpočty mezd minimálně od počátku kalendářního roku do doby jeho úplného uzavření včetně ročního zpracování.

S ohledem na různou požadovanou dobu archivování údajů podle druhu zaměstnaneckého poměru a dle typu dat, musí systém umožnit parametrické nastavení archivačních pravidel pro jednotlivé skupiny údajů a druhy zaměstnaneckých poměrů.

Po uplynutí požadované doby dostupnosti dat v plné šíři záznamů od data ukončení pracovně právního poměru jsou data daného zaměstnance archivována. Archivní záznam zaměstnance musí zůstat on-line dostupný, avšak jeho online data mohou být vhodným způsobem redukována.

Archivní záznamy zaměstnanců musí být dostupné v závislosti na typu dat a odpovídajících zákonných požadavků. Nejdelší požadovaná doba dostupnosti činí 50 let od ukončení pracovně právního vztahu, respektive služebního poměru. Ostatní archivní údaje musí být dostupné v souladu s příslušnými zákony.

##### Zálohování v RPIS

Celý systém a jeho data musí být průběžně zálohována za účelem zajištění obnovitelnosti funkčnosti systému i jeho datového obsahu po případné havárii systému.

Veškerá data v on-line dostupné databázi musí být zálohována za účelem možnosti návratu zpět k datům k určitému časovému okamžiku.

Požadavek vytvářet je:

* měsíční úplné zálohy s životností minimálně 1 rok
* týdenní úplné zálohy s životností minimálně 1 měsíc
* denní zálohy (mohou být úplné nebo diferenciální) s životností minimálně 1 týden.
* zálohy transakčního logu mezi denními zálohami

Zálohy dat musí být pravidelně testovány pro zajištění jejich obnovitelnosti.

V rámci předimplementační analýzy budou ve spolupráci Dodavatele a SPCSS navrženy způsoby předávání informací ze zálohování potřebné pro řešení problémů a analýzy stavu záloh RPIS.

##### Obnovení systému RPIS

Požadovaná doba pro obnovení systému po havárii včetně obnovy dat z poslední dostupné zálohy činí 8 pracovních hodin.

* + 1. SW licence a subskripce

Licence SW na úrovni operačních systémů, virtualizace, zálohování, monitoringu jsou dodávány koncovému zákazníkovi jako součást provozních služeb SPCSS.

Všechny SW produkty nad touto úrovní, potřebné pro vybudování a provoz RPIS, včetně aplikačních serverů, middleware a databází, jsou považovány za součást aplikačního SW a jsou součástí Díla. Seznam těchto produktů poskytne Dodavateli příloha č. 10 Požadavky na technický návrh řešení.

# Role, výkonnost, kapacita, škálovatelnost RPIS

## Role v RPIS

Zadavatel požaduje z hlediska přístupu k RPIS pět uživatelských rolí:

* **Klíčový uživatel** – pracovník personálních odborů nebo zpracovávající mzdovou agendu
* **Aktivní uživatel** – vedoucí zaměstnanec, zadávající do systému požadavky, využívající přehledy a reporting, mající aktivní roli ve schvalovacím workflow
* **Pasivní uživatel** – řadový zaměstnanec (ne vedoucí zaměstnanec), který bude ve velmi omezeném rozsahu do RPIS zadávat data – žádosti
* **Správce OSS –** pracovník OSS, který zpracovává požadavky uživatelů z příslušné OSS a je odpovědný za správnost, úplnost a konzistenci dat ve spravované části systému RPIS. Požadavky, které nejsou řešitelné na jeho úrovni, předává na další úrovně podpory.
* **Administrátor podpory 1. a 2. úrovně –** rozsah oprávnění ke správě RPIS pro tyto role bude řešen v rámci předimplementační analýzy

Dělení počtu uživatelů mezi jednotlivé OSS je následující:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **MF** | **GFŘ** | **GŘC** | **ÚZSVM** | **FAÚ** |
| Klíčový uživatel - HR, mzdy | 40 | 210 | 86 | 34 | 4 |
| Aktivní uživatel - vedoucí pracovník | 200 | 2266 | 658 | 254 | 1 |
| Pasivní uživatel - ostatní zaměstnanec | 1650 | 14034 | 5515 | 1536 | 59 |
| Správce OSS | 1 | 1 | 2 | 1 | 1 |

**Počet uživatelů pro roli Administrátor podpory 1. a 2. úrovně v SPCSS – 5 osob**

## Výkonnost a kapacita RPIS

Odezva systému na běžné akce uživatelů (jednoduchá vyhledávání, založení záznamu, editace záznamu apod.) by měla být následující:

- do 1 sekundy min. v 80 % případů

- do 2 sekund max. ve 20 % případů

- do 5 sekund max. ve 2 % případů

Odezva systému na náročnější akce uživatelů (složitější vyhledávání, komplexnější výstupní sestavy, jednodušší dávková zpracování) by měla být následující:

- do 10 sekund min. v 80 % případů

- do 30 sekund max. ve 20 % případů

- do 60 sekund max. ve 2 % případů

Doba měsíčního zpracování mezd by měla být v závislosti na počtu zpracovávaných kmenových záznamů:

- do 10 minut pro FAÚ

- do 20 minut pro GŘC, MF, ÚZVSM

- do 30 minut pro GFŘ

Návrh architektury, která splní výše uvedené parametry pomocí stavebních bloků SPCSS definovaných v kapitole 1.6 Standardy a stavební bloky.

# Požadavky na bezpečnost

## Obecné požadavky na bezpečnost

Nabízený systém musí naplnit požadavky vyplývající ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti pro prvek významné infrastruktury (VIS). Systém řízení bezpečnosti musí být navržen a implementován v souladu s normami řady ISO/IEC 270xx (včetně rozšiřující normy ISO 27552), ISO 29151, ISO 29100:2011, a systém řízení provozu a správy RPIS musí být navržen a implementován v souladu s normou ČSN ISO/IEC 20000.

Pokud bude systém podporovat klienta nebo jiné rozhraní pro uživatele typu řadový / vedoucí zaměstnanec na mobilních platformách bez zabezpečení VPN, musí být způsob zabezpečení dat na těchto platformách v souladu s interními předpisy správce a provozovatele systému a platnou legislativou (např. splnění podmínek bezpečnostní dokumentace ohledně BYOD, BYOC nebo GDPR).

Součástí údajů vedených v RPIS budou údaje klasifikované dle zákona o ochraně osobních údajů jako:

* osobní údaje
* citlivé údaje

Systém nebude obsahovat údaje klasifikované dle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti a nebude obsahovat žádné údaje charakterizované jako obchodní tajemství.

Systém musí naplnit všechny požadavky vyplývající ze zákonů a dalších právních předpisů v souvislosti s kvalifikací systému a obsažených údajů.

Při zajištění dodávky RPIS je požadována součinnosti Dodavatele se Zadavatelem při zpracování typového bezpečnostního projektu v souladu s uznávanými pravidly a normami, vytvořený pro konkrétní navržené technické řešení.

V rámci bezpečnostního projektu bude vypracováno minimálně následující:

* identifikace a hodnocení aktiv,
* identifikace a hodnocení rizik,
* plán zvládání rizik,
* doporučená bezpečnostní opatření,
* scénář pro pravidelné prověřování účinnosti bezpečnostních opatření a jejich dodržování,
* scénář pro testy zranitelnosti.

RPIS musí být odolný proti známým bezpečnostním hrozbám a útokům z vnějších i vnitřních sítí.

RPIS a jeho dokumentace musí vyhovovat požadavkům legislativy GDPR a eIDAS.

## Návrh řešení bezpečnosti

Návrh řešení bezpečnosti musí být v souladu se vstupy a požadavky definovanými v kapitole 4.3 CKB, SOC a bezpečnostní monitoring. Dodavatel navrhne a popíše řešení bezpečnosti v příloze č.10 Požadavky na technický návrh řešení.

# Logování, provozní a bezpečnostní monitoring

## Popis provozního monitoringu Zadavatele

SPCSS jako Zadavatel poskytuje dohled infrastruktury v režimu 7x24 v podobě proaktivního monitoringu stavu serverů a datových sítí na různých úrovních, včetně měření Service Level Agreement (dále jen „SLA“). Systém provozního monitoringu je integrován s aplikací Service Desk Manager SPCSS, která zajistí řešení událostí v rámci procesů Incident managementu a Request Fulfillment.

SPCSS používá nástroje provozního monitoring od firmy CA. SW licence pro monitoring systému jsou součástí služby SPCSS.

Přímý přístup Dodavatele do nástrojů provozního monitoringu není standardně poskytován, primární nástroj pro komunikaci s Dodavatelem je Service Desk SPCSS. V rámci předimplementační analýzy budou ve spolupráci Dodavatele a SPCSS navrženy způsoby předávání informací z monitoringu potřebné pro řešení problémů a analýzy stavu RPIS.

## Požadavky na provozní monitoring RPIS

Dodavatel navrhne systém logování aplikací a SW produktů dle bezpečnostních a provozních požadavků Zadavatele v souladu s jeho bezpečnostními a provozními požadavky. Návrh a integrace RPIS do provozního monitoringu Zadavatele je požadován v takovém rozsahu, aby bylo možné monitorovat provozní stavy systému a plnění parametrů SLA. Dodavatel bude se Zadavatelem spolupracovat na analýze dohledových metrik a návrhu a implementaci metrik na úrovní aplikace, SW produktů a dat a zajistí jejich integraci do monitorovacích nástrojů Zadavatele. Součástí implementace monitoringu je naplnění konfigurační databáze (CMDB).

Detailní požadavky na provozní monitoring budou součástí předimplementační analýzy.

## Popis bezpečnostního monitoringu (CKB a SOC) Zadavatele

Služby centra kybernetické bezpečnosti (CKB) a Security operation centra (SOC) zajišťují provozní služby kybernetické bezpečnosti systémů a sítí v souladu se standardy ČSN ISO/IEC 27000 a Zákonem o kybernetické bezpečnosti (ZKB), včetně detekce, řešení a hlášení bezpečnostních incidentů. Součástí standardních služeb SPCSS v oblasti bezpečnostního monitoringu je i dohledový systém typu SIEM, který odpovídá požadavkům zákona 181/2014 Sb. na úrovni kritické informační infrastruktury (SPCSS jako podnik je prvkem KII).

SW licence systému bezpečnostního monitoringu jsou součástí služby SPCSS. Část návrhové, implementační a provozní dokumentace CKB a bezpečnostního monitoringu služeb a aplikací je chráněna v režimu utajovaných informací stupně Vyhrazené dle Zákona o ochraně utajovaných informací.

## Požadavky na bezpečnostní monitoring RPIS

Je požadována integrace RPIS do systému bezpečnostního monitoringu Zadavatele. Vlastní implementaci bezpečnostního monitoringu provede Zadavatel. Dodavatel ve spolupráci se Zadavatelem provede analýzu hrozeb. Dodavatel navrhne a implementuje metriky bezpečnostního monitoringu na úrovni aplikace, SW produktů a dat a společně se Zadavatelem zajistí jejich integraci do monitoringových nástrojů Zadavatele. Integrace bezpečnostního monitoringu na úrovni aplikace, SW produktů a dat bude provedena formou logování.

# Autentizace a autorizace

Každý uživatel systému musí být pro přístup do systému řádně autentizován.

V případech, kdy nelze uplatnit SSO autentizaci (např. komunikace s externími systémy), je požadována autentizace vícefaktorová – tj. systém zvládá, nebo je schopen integrovat vícefaktorovou autentizaci pomocí elektronického certifikátu nahraného např. na ID kartě zaměstnance.

Ve výjimečných případech (nouzové / dočasné řešení apod.) je možné použít základní autentizaci uživatelským jménem a heslem za předpokladu dodržení následujících pravidel:

* komunikace musí probíhat pomocí zabezpečeného kanálu (min. HTTPS protokol),
* je požadováno ověřování proti záznamům v AD přes LDAP (ne vlastní správa hesel uživatelů v systému),

 nebo

* musí být umožněno nastavení a vynucení politiky hesel na odpovídající úrovni.

Systém musí umožnit omezení horizontálního přístupu k datům (viditelnost / modifikace záznamů) na úrovni konkrétního uživatele, minimálně na základě těchto kritérií:

* zajištění unikátnosti uživatele minimálně na úrovni rezortu
* osobní číslo - vlastní data pro uživatele typu zaměstnanec,
* organizační struktura - data podřízených pro uživatele typu vedoucí na každém stupni,
* přiřazení pracovníka k uživateli / skupině uživatelů dle organizační struktury - na úrovni standardního uživatele,
* přiřazení pracovníka k uživateli / skupině uživatelů dle regionální příslušnosti bez ohledu na organizační strukturu - tzv. plátcovy pokladny.

Systém musí umožnit dočasné přidělení uživatelských oprávnění jednoho uživatele uživateli druhému pro případ zastupování. Toto oprávnění může být předáno pouze uživateli se stejnou rolí.

Při dočasném přidělení uživatelských oprávnění uživatel nesmí přijít o svá běžná uživatelská oprávnění. Systém musí být připraven k napojení na externí systém pro správu identit a uživatelských oprávnění (IDAM = Identity and Authorization Management System), který je jiný a samostatný pro každou OSS a měl by podporovat otevřené datové rozhraní pro výměnu autorizačních dat. Systém musí být zároveň připraven k napojení (a přechod) na plánovaný nový centrální LDAP. Metodické požadavky, které vzejdou z nastavení dle výše uvedeného, budou předmětem předimplementační analýzy.

# Důvěrnost a integrita

Systém musí umožňovat zajištění důvěrnosti a integrity dat na úrovni DB stroje, a to i před správci provozního prostředí. Vzhledem k nutnosti dostupnosti dat pro potřeby jejich zpracování DB serverem (zpracování dat na úrovni DB procedur, řazení dat DB serverem apod.) se nepředpokládá externí šifrování dat. Z toho vyplývá požadavek na využití DB stroje, který zajistí možnost šifrování dat přímo v databázi.

Pokud se chráněná data vyskytují ve filesystému (sestavy, datové soubory, záznamy o činnosti apod.), musí být odpovídajícím způsobem zajištěna jejich důvěrnost a integrita (např. šifrováním) na všech architektonických vrstvách systému, a to i před správci provozního prostředí.

Systém musí zajistit důvěrnost a integritu dat na celé cestě mezi databázovým serverem a klientem, tedy je požadováno zabezpečené propojení mezi všemi architektonickými vrstvami systému.

Zvláštní pozornost je v této oblasti třeba věnovat komunikacím s okolními systémy, vzdáleným přístupům prostřednictvím veřejných sítí, přístupům na bázi bezdrátových technologií a mobilních klientů.

Důvěrnost a integrita dat musí být zachována i při zálohování a archivaci, a to jak při vlastním procesu, tak i následně vzhledem k médiím, na nichž jsou zálohy a archivní data uloženy.

Specifickou pozornost je třeba věnovat též řešení důvěrnosti a integrity dat při jejich převodu ze stávajících systémů. Pokud z objektivních / technických důvodů nebude možné zajistit náležitou úroveň zabezpečení prostřednictvím technických opatření, bude nutné zranitelná místa řešit opatřeními organizačními, která budou navržena Dodavatelem ve spolupráci se Zadavatelem.

# Auditovatelnost a nepopiratelnost

Všechny úspěšné i neúspěšné přístupy k systému musí být logovány. Záznamy o neúspěšných přístupech musí být monitorovány a v případě zvýšeného počtu neúspěšných pokusů se požaduje vyvolání odpovídající akce. Veškeré změny dat v systému musí být logovány tak, aby bylo možné zjistit kdo, kdy, jak a která data v systému modifikoval:

* u nově založených záznamů (operace INSERT) musí být možno dohledat informace kdo, kdy a v jakém stavu (obsahu dat) záznam založil;
* u změněného záznamu (při každé operaci UPDATE) musí být umožněno zjištění kdo, kdy a jakým způsobem data změnil;
* u smazaného záznamu nesmí dojít k trvalému odstranění dat („nepodporovat operaci DELETE“), ale pouze k logickému zneplatnění záznamu (provést operaci UPDATE) a musí být zaznamenáno kdo, kdy a v jakém stavu dat záznam logicky zneplatnil.

Ze záznamů musí být možné zrekonstruovat kompletní historii každého datového objektu včetně časové specifikace jeho změn, včetně historie všech datových vazeb na ostatní datové objekty. Ke každé změně dat musí být možné identifikovat jejího původce (uživatel / systém). U některých osobních / citlivých údajů musí být možné zaznamenávat též aktivity uživatelů související s pasivním přístupem k datům (operace SELECT), tedy pouhé jejich zobrazení, vytvoření sestavy, datový export, přístup přes datové rozhraní.

Dále musí být zaznamenáno nejen kdo, kdy a k jaké datové entitě přistupoval, ale také ke kterým konkrétním datovým objektům (řádky a sloupce entity) uživatel přistupoval (mohou být poznamenána též konkrétní data (datový obsah), která si uživatel zobrazil, avšak není to nutné vzhledem k možnosti rekonstrukce obsahu datových objektů k danému času). Pravidla pro ukládání záznamů o přístupech a činnosti specifikované pro uživatele je nutné přiměřeně uplatnit i pro činnost okolních systémů přistupujících k RPIS prostřednictvím nějakých rozhraní. Systém musí umožnit parametrické konfigurování pro jednotlivé auditované prvky. Požaduje se, aby záznamy o činnosti byly logovány a zaznamenány a systém musí umožnit tyto záznamy uložit do externího nástroje typu SIEM, a to dle kapitoly 4.3 této přílohy.

Všechny záznamy o činnosti v RPIS musí být zabezpečeny proti:

* neoprávněnému přístupu k datům (zachování důvěrnosti);
* neoprávněné manipulaci (zachování integrity a prokazatelnosti, resp. principu nepopiratelnosti);
* ztrátě uložených informací v požadované době dostupnosti záznamů (zálohování a archivace).

Přístup k záznamům o činnosti musí být umožněn pouze oprávněným osobám (nemusí být administrátoři daného provozního prostředí). Za účelem naplnění těchto požadavků musí být cílové prostředí vybaveno technologiemi, které umožní šifrování záznamů o činnosti a automatické odkládání jejich kopií do prostředí, kde nebude možná jakákoliv manipulace s nimi. Systém musí umožňovat vyhodnocování činnosti uživatelů / systémů a detekci nestandardních stavů, jako např.:

* zvýšený počet neúspěšných pokusů o přístup k systému,
* zvýšený počet čtení / zápisů dat oproti běžnému stavu, resp. probíhajícímu typu zpracování,

apod.

V případě nestandardních stavů musí být vyvolána odpovídající akce:

* varování správce systému o nestandardním stavu,
* výstup vyhodnocení, resp. detekce nestandardních stavů do externích logovacích/monitorovacích systémů.

Systém musí umožnit ukládání logů a auditních záznamů externě (mimo IS) v centrálním úložišti logů.

Systém musí umožnit konkrétnímu uživateli prokázat jím provedené běžné akce na základě vlastností popsaných v požadavcích z oblasti auditovatelnosti.

Pro běžné akce tedy není explicitně požadována nepopiratelnost na úrovni elektronického podepisování každé datové změny. Nepopiratelnost (ale též další bezpečnostní požadavky) některých výstupů ze systému musí být zajištěna použitím zaručeného elektronického podpisu s využitím kvalifikovaných elektronických zabezpečovacích prvků elektronických dokumentů.

Systém musí umožnit požadované výstupy podepisovat zaručeným podpisem buď přímo vlastními prostředky RPIS, nebo prostřednictvím automatického volání prostředku zajišťujícího přiložení zaručeného elektronického podpisu v externím systému.

# Rozhraní systému

Nový RPIS by měl podporovat datové rozhraní pomocí otevřených technologií a standardů (jako například XML, webové služby, apod.). Rozhraní musí umožnit uživatelsky řídit tvorbu konkrétních výstupů na bázi otevřeného datového rozhraní (například možnost definovat konkrétní metodu webové služby, která poskytne vybraná data o vybraných entitách). Datové rozhraní musí splňovat bezpečnostní požadavky z oblastí autentizace, autorizace, důvěrnosti a integrity dat, auditovatelnosti a nepopiratelnosti. Dodavatel popíše navrhovaný způsob řešení bezpečnostních požadavků pro otevřená datová rozhraní. Stejný popis předloží pro klienta nebo jiné rozhraní pro uživatele typu řadový / vedoucí zaměstnanec na mobilních platformách bez zabezpečení VPN.

Jsou požadovány formáty výstupních sestav, které budou snadno uchopitelné v prostředí zúčastněných organizací. Zejména se jedná o přenositelné a otevřené formáty (ODF, PDF a další) a formáty Microsoft Office (XLSX, DOCX a další). Je požadována možnost exportu dat z výstupních sestav nebo přímá tvorba datového výstupu namísto sestavy, a to do některého z otevřených standardních datových formátů (CSV, XML, TXT apod.). Veškeré výstupy dat z RPIS budou chráněny přístupovými právy.

Nový RPIS by měl umožnit uživatelskou tvorbu výstupních sestav (generátor sestav). Je požadována uživatelská přívětivost a nízká náročnost tvorby sestav, která nebude vyžadovat žádné specifické programátorské schopnosti a znalosti. Generátor sestav by měl umožňovat vytvářet jak textové, tak i grafické objekty (grafy, tabulky, diagramy) a uživatelskou definici grafické podoby sestavy (layout).

Nový RPIS musí umožnit realizovat všechny potřebné vazby na okolní systémy. V praxi se jedná jak o kompletní náhradu všech existujících vazeb stávajících RPIS na okolní systémy, tak i o požadavky na realizaci vazeb nových. Vazby na okolní systémy budou realizovány ve všech cílových organizacích. Okolní prostředí RPIS v rámci jednotlivých organizací je různorodé s částečnými společnými prvky. Model požadovaných vazeb RPIS na okolní systémy je pro každou organizací samostatný.

Pokud se však vyskytuje vazba na tentýž systém ve více organizacích, měla by být ve všech takových organizacích implementována totožně. Vazby na okolní systémy budou postaveny na otevřeném datovém rozhraní. Vždy musí být respektovány též možnosti spolupracujícího systému. Konkrétní specifikace požadovaných vazeb na okolní systémy jsou uvedeny v rámci funkčních požadavků na nový systém.

# Podpora, provoz a údržba, klasifikace chyb

## Definice provozní podpory RPIS

Provozní podpora bude zajišťována pro všechny organizace v resortu, kterým je poskytována služba RPIS. Podpora se dělí celkem na čtyři úrovně, jejichž odpovědnosti jsou definovány v následujících kapitolách. Úrovně L1, L2 a L3 se týkají Zadavatele a Dodavatele systému RPIS. Úroveň L0 se týká jednotlivých OSS (správců dat).

## Podpora nulté úrovně (L0)

Podpora nulté úrovně je zajišťována rolí správce a metodikem OSS pro uživatele vlastní OSS. Řeší metodické problémy specifické pro danou OSS, filtruje požadavky uživatelů a předává dále požadavky, které mají být řešeny SPCSS nebo Dodavatelem. Dodavatel navrhne způsob podchycení požadavků v rámci OSS a jejich oddělení od režimu SD pro 1. ,2. a 3. úrovně podpory.

Požadavky 0. úrovně nepodléhají SLA.

## Podpora první úrovně (L1)

Podpora první úrovně zahrnuje přímou komunikaci s uživateli, příjem a evidenci hlášení incidentů a požadavků a řešení nejjednodušších a nejběžnějších problémů v systému.

Podpora první úrovně bude řešena pomocí nástroje Service Desk a Call Centra SPCSS a zajišťuje ji SPCSS.

Požadavky uživatelské podpory, které nebudou řešitelné podporou první úrovně, budou předávány na podporu druhé úrovně.

## Podpora druhé úrovně (L2)

Podpora druhé úrovně zahrnuje analýzu a řešení incidentů a požadavků na provozní součinnost, které nevyžadují změny nastavení ani zdrojového kódu a jsou řešeny proškoleným specialistou.

Podpora druhé úrovně bude řešena pomocí nástroje Service Desk SPCSS a zajišťuje ji SPCSS.

* Podpora druhé úrovně řeší incidenty a požadavky nejběžnějších činností, které v systému provádí klíčoví uživatelé, a nejsou řešitelné rolí Správce OSS.

Pracovníci podpory druhé úrovně postupují na základě procesů a informací obsažených v provozní dokumentaci Díla. Pracovníci podpory druhé úrovně mají během období post-implementační podpory na pracovišti SPCSS k dispozici zástupce provozní podpory v pracovních hodinách systému po dobu 3 měsíců za účelem poskytnutí zvýšené podpory systému a vyškolení pracovníků první a druhé úrovně podpory SPCSS.

Požadavky uživatelské podpory, které nebudou řešitelné podporou druhé úrovně, budou předávány na podporu třetí úrovně.

## Podpora třetí úrovně (L3)

Podpora třetí úrovně zahrnuje analýzu a řešení incidentů a požadavků na provozní součinnost, které vyžadují změny, znalost zdrojového kódu, konfigurace a hlubokou znalost systému i jeho architektury. Podpora třetí úrovně zahrnuje aktualizaci provozní dokumentace pro podporu druhé úrovně.

Podporu třetí úrovně zajišťuje Dodavatel.

Dodavatel zajistí telefonickou podporu pro řešení incidentů a požadavků, která bude využívána pracovníky L1 a L2 podpory k operativnímu informování a řešení požadavků. Provozní doba telefonické podpory Dodavatele odpovídá provozní době systému.

Plnění smluvních SLA Dodavatele souvisejících s poskytováním L3 podpory bude vyhodnocováno na základě údajů zaznamenaných v nástroji Service Desk SPCSS.

Pro spolupráci s L3 podporou za účelem řešení vzniklých incidentů a požadavků je možné provést

1. integraci Service Desk SPCSS se Service Deskem Dodavatele, a to formou webové služby, za účelem předávání ticketů k řešení

nebo

1. poskytnutí přístupu do Service Desku SPCSS řešitelům L3 podpory Dodavatele.

Návrh a implementace integrace musí být obsaženy v ceně řešení Dodavatele.

Přístup pracovníků SPCSS L1 a L2 podpory do nástrojů na evidenci incidentů a požadavků Dodavatele se nepředpokládá.

## SLA podpory první úrovně (L1) a Service Desk

* + 1. Provozní doba

Provozní doba první úrovně podpory je 5x10, a to od 8 do 18 hodin.

* + 1. Reakční doba

Reakční doba je čas od nahlášení incidentu do přijetí k řešení pracovníkem L1 podpory.

Reakční doba v provozní době systému je 15 minut.

## SLA podpory druhé úrovně (L2)

* + 1. Provozní doba

Provozní doba druhé úrovně podpory je 5x10, a to od 8 do 18 hodin.

* + 1. Reakční doba

Reakční doba je čas od přidělení incidentu do přijetí k řešení pracovníkem L2 podpory.

Reakční doba pro podporu druhé úrovně není specifikována.

## SLA podpory třetí úrovně (L3)

* + 1. Provozní doba

Provozní doba třetí úrovně podpory je 5x10, a to od 8 do 18 hodin.

* + 1. Reakční doba

Reakční doba je čas od přidělení incidentu do přijetí k řešení pracovníkem L3 podpory.

Reakční doba pro podporu třetí úrovně není specifikována.

* + 1. Doba opravy

Doba potřebná pro vyřešení chyb se počítá od času nahlášení chyby do jejího vyřešení v provozní době systému. Vyřešení může být úplné nebo formou náhradního řešení. Doby vyřešení jsou stanoveny následujícím způsobem:

1. Kritická chyba: 10 hodin
2. Závažná chyba: 40 hodin
3. Drobná chyba: 100 hodin

## Klasifikace chyb

Detailní popis chyb dle výše uvedené klasifikace:

1. Kritická chyba nastává, pokud nastane minimálně jedna z níže uvedených skutečností:
* totální výpadek systému;
* vyžadován restart systému;
* obnova informačního systému RPIS ze zálohy;
* nefunkčnost takového charakteru, že zpracování předepsaných dokumentů musí být zajištěno náhradním řešením (manuálně, kombinací manuálního a strojového zpracování dat apod.);
* nesoulad některé funkce RPIS s legislativními požadavky.
1. Závažná chyba nastává, pokud nastane minimálně jedna z níže uvedených skutečností, avšak chyba není charakterizována jako kritická:
* nefunkčnost / nedostupnost některé dílčí funkcionality;
* nesoulad dílčích výsledků zpracování dat s očekávanými výsledky.
1. Drobná chyba
* všechny ostatní chyby (např. chybný popisek, pravopisná chyba v textech, chybné formátování, vzhledový nedostatek apod.).

# Rozvojové požadavky na RPIS – Služby rozvoje

Po celou dobu provozu RPIS (10 let) je požadována realizace nových uživatelských a technických rozvojových požadavků (technický rozvoj systému), které budou rozšiřovat nebo měnit funkčnost systému nad rámec funkčních a nefunkčních požadavků vymezených v zadávací dokumentaci.

## Objednávání Služeb rozvoje

Tato kapitola obsahuje základní pravidla objednávání řízení a vypořádání Rozvojových požadavků.

Rozvojové požadavky jsou objednávány oprávněnou osobou Zadavatele, která zašle oprávněné osobě Dodavatele poptávku emailem nebo jiným písemným způsobem.

Poptávka minimálně obsahuje:

1. Specifikaci požadovaných Rozvojových požadavků
2. Požadovaný termín realizace Rozvojových požadavků
3. Požadovaný termín předložení nabídky

Dodavatel v požadovaném termínu předloží emailem nebo jiným písemným způsobem nabídku k Rozvojovým požadavkům, která bude obsahovat:

1. Způsob řešení poptávky
2. Termín realizace Rozvojových požadavků
3. Odhad náročnosti vyjádřený v člověkodnech nebo jeho částech
4. Požadovanou součinnost Zadavatele
5. Rizika realizace Rozvojových požadavků a způsoby jejich snížení

Zadavatel je oprávněn požadovat po Dodavateli upřesnění nebo doplnění nabídky Rozvojových požadavků, a to i opakovaně.

Souhlasí-li Zadavatel s nabídkou Dodavatele, zašle Dodavateli objednávku, která bude obsahovat:

1. Specifikaci požadovaných Rozvojových požadavků
2. Požadovaný termín realizace Rozvojových požadavků
3. Kapacitní náročnost
4. Specifikaci součinnosti Zadavatele
5. Specifikaci případných ostatních povinností Dodavatele

## Akceptace Služeb rozvoje

Po splnění Rozvojových požadavků je Dodavatel povinen předložit Akceptační protokol s výkazem skutečně odpracovaných člověkodní nebo jejich částí. Počet člověkodní v Akceptačním protokolu nesmí překročit počet člověkodní z nabídky Rozvojových požadavků. Součástí akceptačního protokolu je dokumentace úprav systému případně zdrojový kód.

# Školení

## Školení metodických pracovníků OSS

Dodavatel zajistí uživatelská školení Klíčových uživatelů a Správců OSS pro tyto počty frekventantů:

MF – 40 Klíčových uživatelů, 1 Správce OSS

GFŘ – 210 Klíčových uživatelů, 1 Správce OSS

GŘC – 86 Klíčových uživatelů, 2 Správci OSS

ÚZSVM – 34 Klíčových uživatelů, 1 Správce OSS

FAÚ – 4 Klíčoví uživatelé, 1 Správce OSS.

Školení budou probíhat v kurzech v rozsahu dvou pracovních dnů, vždy pro skupinu 10 frekventantů. Frekventanti obdrží po absolvování školení učební materiály obsahující náplň školení. Všechna školení budou probíhat v Praze v prostorách Zadavatele. Termín školení bude upřesněn v rámci tvorby realizačního harmonogramu v průběhu JŘSU.

Pro funkcionality pokrývající činnosti Aktivního uživatele a Pasivního uživatele bude k dispozici příslušná dokumentace a video nápověda přístupná z prezentační vrstvy systému (portálu).

## Školení administrátorů první a druhé úrovně podpory

* + 1. Školení administrátorů první úrovně podpory
* Základní architekturu modulů personálního systému
* Základní konfiguraci modulů personálního systému
* Používané postupy v nejběžnějších problémech uživatelů z následujících oblastí:
* Řízení uživatelských přístupů a hesel
* Obecné postupy v jednotlivých oblastech personálního systému (např. seznámení s databází známých chyb systému, best-practices postupů, manuál pro pracovníky service desk, apod.)
* Rozsah školení 2 pracovní dny pro 5 pracovníků.
	+ 1. Školení administrátorů druhé úrovně podpory
* Základní architekturu modulů personálního systému
* Základní konfiguraci modulů personálního systému
* Technická realizace business procesů v RPIS v jednotlivých modulech z následujících oblastí
* Oblast Personalistika
* Zavedení zaměstnance do RPIS
* Změna osobních údajů
* Zadání dosavadní praxe pro zápočet a zařazení zaměstnance do platového stupně
* Práce a mzdy
* Zadání platových nároků
* Výpočet platu
* Zadání nepřítomností
* Měsíční zpracování výplat
* Přehled o uzávěrkových operacích za zpracovávaný měsíc
* Přehled o sestavách pro účtárnu a vytvoření příkazů pro banky pro platy a povinné odvody
* Opravy historických záznamů (pro chybná zadání, zpětně přiznané nároky)
* Práce s evidenčními a mzdovými listy
* Znalost vazeb na zdravotní pojišťovny, SSZ a hlášení na RNP
* Znalost ročního zúčtování daní za zaměstnance
* Obecná znalost práce se sestavami
* Znalost zpracovávání povinného podílu zaměstnávání osob se zdravotním postižením
* Rozsah školení 2 pracovní dny pro 5 pracovníků

# Další požadavky

## Migrace

Dodavatel navrhne rozhraní a postupy pro migrace dat ze stávajících systémů OSS a popíše nezbytnou organizační a technickou součinnost, již bude potřebovat. Data zahrnují jak podklady pro číselníky nutné pro provoz nového systému, tak historická data, jejichž uchování je dáno platnou legislativou. Pro každou OSS je nezbytné zajistit bezpečnost a důvěrnost vlastních dat. Požadavky jednotlivých OSS na migraci dat do nového systému jsou uvedeny níže.

* + 1. Ministerstvo Financí

Ministerstvo Financí požaduje převést do nového systému:

PAM (práce a mzdy)

Z PAM je nezbytné převést data z formulářů:

F1, F2, F3, F4, F5, F9, F11, F12, F13, F15, F17, F18, F19, F20, F21, F22, F23, F24, F26, F27, F28, F81, F94, F97, F115, EVCIZY, SRAZKYH.

Kmenové soubory výsledků: F 30 – F49 (jedná se o formuláře s veškerými mzdovými údaji)

Kompletní převod Tabulek s historií (formuláře s organizační strukturou a rozborovými hledisky).

ELD, RNP, KZP (elektronické podání registr nemocenského pojištění, komunikace se zdravotními pojišťovnami)

Všechny odeslané dávky.

PER (personalistika)

Celé věty:

a) s aktivními zaměstnanci obsahující: osobní + doplňující údaje, adresy, spojení, průkazy, vzdělání, zkoušky a osvědčení, evidence důchodů + kompletní historie pracovního zařazení, smluv, dokumentů, platového zařazení, vynětí, zastupování, lékařské prohlídky, dohody o odpovědnosti, povolení podnikatelské činnosti, změny státní služby a opatření zaslaná do ISoSS. Kompletní formulář odmatre.

b) s odešlými zaměstnanci za posledních 10 let.

STM (systemizace)

Kompletní historie organizačních útvarů – TUTV a míst TSMV, včetně všech poznámek a rezervací.

VZD (vzdělávání)

Z VZD převod formulářů:

Osobyx, pzarazx, smlouvax, utajenix, vyneti, znalostx, vsmkrit – společné formuláře s PER.

Prumvyd, kompx, planvzdx, akcepozx, akceplpx, hakce, profesx, uprakcex, vnaklax, vzdpreh, takce, menuakce, toblastv, lektori, lekpzar, lekodb, tlodb.

Kompletní formuláře vzdělávací akce + přehledy vzdělávacích akcí.

ISS (Informační systém státní služby)

Přehled odeslaných dávek s výsledkem za poslední rok.

WKF (workflow)

Plány dovolených za poslední 2 roky, všechny návrhy odměn.

CAF (zaměstnanecké výhody)

Kompletní věty s čerpáním limitu za 3 roky.

* + 1. GFŘ

GFŘ požaduje převést do nového systému:

* Celou oblast PER (personalistika - údaje o zaměstnancích)
* Oblast PAM (Mzdy)
* data za mzdy za celý aktuální rok, předběžně od 1.1.2018
* PAM historii od roku 2011 do současnosti

Požadovaná data z personálního systému – z archivních aplikací IS VEMA jsou požadovány níže uvedené sestavy ve formátu využívaném exportem MEL, případně Excel:

* S 148 mzdový list
* S 109 příloha mzdového listu
* S 86 evidenční listy
* S 91 potvrzení zaměstnavatele o výši příjmu (za celý rok, od roku 2001 do roku 2012)
* S 30 potvrzení o zdaněné mzdě
* S 45 potvrzení o zaměstnání
* S 50 roční zúčtování daně

Z modulů RNP, komunikace se zdravotní pojišťovnou a ČSSZ a systém u ISSOS – historie podání v co možná největším rozsahu (možno použít Excel, mimo PER)

Data z PIS za STM (systemizace)

Převést kompletní STM včetně historie – tj. data o místech, útvarech, vzorech – s tím související veškerá data v číselnících (TOJRED, TSKUPUT, TUFP, TLOK) a v podčíselnících – obory státní služby, katalog prací, katalog správních činností, lokalita, funkce, obsazenost (souvisí s PER), jazykové znalosti, utajené informace, atd.

Oddělení vzdělávání požaduje následující oblasti:

* převod všech aktuálních i historických dat, včetně statistických souborů,
* převod číselníků vzdělávání,
* zachování veškeré funkčnosti včetně recepce ve VZ, vazby na vzdělávací zařízení a rozdělení kompetencí k jednotlivým větám některých souborů, přístupům k potřebným souborům a číselníkům v PER, PAM a STM,
* zachování stávajících sestav.
	+ 1. GŘC

GŘC požaduje migrovat kompletní data ze stávajícího systému Odyssea, a to z následujících oblastí:

Oblast Personalistika – veškerá personální data o současných i bývalých zaměstnancích CS ČR, včetně historie:

* Základní údaje o osobě (jméno, příjmení, datum narození, rodné číslo, rodinný stav, místo narození, občanství, …)
* Adresy (trvalé, přechodné, kontaktní, …)
* Informace o rodinných příslušnících
* Sociální pojištění
* Zdravotní pojišťovna
* Platby mimo MÚ (penzijní spoření, atd.)
* Důchody a ZPS
* Vzdělání a další znalosti
* Další údaje jako jsou: hmotná odpovědnost, závazky k organizaci, sídlo pracoviště, tel. a ostatní spojení
* Kázeňské odměny
* Kázeňské tresty
* Lékařské prohlídky
* Psychologická vyšetření
* Benefity zaměstnance
* Hodnocení
* Údaje vztahující se k PPV:
* Funkce
* Organizační zařazení
* Pracovní vztah a pracovní doba
* Dovolená
* Zápočty dob zaměstnání
* Průběh zaměstnání
* Stupnice
* Nástupy a výstupy
* Příznaky PPV
* Evidenční stav
* Další údaje (udělování výjimek, sídlo pracoviště)
* Výstrojní norma

Oblast Systemizace - veškerá systemizační data - existují dvě varianty systemizačního stromu, tj. do 1.1.1998 do 31.12.2012 a současná varianta platná od 1.1.2013

* Základní informace o místech (číslo místa, název místa, funkce, % využití, kategorie, třída, organizační zařazení, sídlo pracoviště, …) včetně historie
* Historie osob na místech
* Historie nadřízených
* Důvody vzniku a zániku místa
* Popisy:
* Vlastnosti - fyzická způsobilost, zdravotní způsobilost, stupeň utajení, katalogová činnost
* Znalosti a dovednosti – jazykové znalosti
* Klíčové ukazatele výkonu - zvláštní příplatky
* Výstrojní norma

Oblast Ekonomiky práce – veškerá data včetně historie

* Mzdové zařazení a příplatky
* Platový tarif
* Osobní příplatek
* Zvláštní příplatek
* Příplatek za vedení
* Limity a čerpání (přesčasové hodiny)

Oblast Mzdy – veškerá data včetně historie

* Veškeré výpočty platů
* Veškeré výpočty výsluh

Oblast Vzdělávání – veškerá data včetně historie

* Kurzy a vzdělávací akce

Oblast Sociální fondy

* Evidence poskytnutých rekreací
* Čerpání dotací FKSP

S výše uvedenými daty jsou spojené číselníky, které je nutno do migrace zahrnout.

* + 1. ÚZSVM

Oblast Personalistika

* převod všech personálních dat včetně personálních dokumentů s historií.

Oblast Mzdy

* kompletní převod dat nutných pro budoucí zpracování mezd a kompletní historii mezd pro analytické účely.

Oblast Systemizace

* kompletní převod dat systemizace (organizační strukturu, popisy míst, požadavky na kvalifikaci atd.)

ÚZSVM požaduje:

* zajistit dodávku tabulek ve formátu Excel, vybavené metadaty s popisy sémantických dat požadovaných pro převod ze stávajícího řešení
	+ 1. FAÚ

Požadována migrace veškerých dat vzniklých a pořízených v rozsahu od 1. 1. 2017 ze všech modulů stávajícího PIS.

|  |  |  |  |
| --- | --- | --- | --- |
| V | [místo] | dne | [DD.MM.RRRR]  |
|  |
| [název dodavatele][jméno a příjmení osob/y oprávněné jednat za dodavatele, včetně titulu opravňujícího k zastupování] |