**Studie proveditelnosti projektu „Výstavba, implementace
a technická podpora ICIS OZP“**

**Příloha P05B**

**Seznam požadavků – Servis - Technologie**

Datum: 28. 11. 2013

Počet stran: 8

**Obsah**

[1 Číselníky a konfigurace interních parametrů informačního systému (SPC) 3](#_Toc374038058)

[2 Administrace (ADM) 4](#_Toc374038059)

[3 Bezpečnost (BZP) 5](#_Toc374038060)

[4 Autentizace a identity management (AIM) 6](#_Toc374038061)

[5 Pořizovací programy (POP) 7](#_Toc374038062)

[6 Systém varování (SVA) 8](#_Toc374038063)

# Číselníky a konfigurace interních parametrů informačního systému (SPC)

| Kód | Název požadavku | Detailní popis požadavku | Související proces |
| --- | --- | --- | --- |
| ST-SPC-000 |  | Systém umožní přijetí a nahrání externích číselníků do systému včetně individuálních úprav. | ST-SPC |
| ST-SPC-001 | Nahrání externího číselníku | Umožnit nahrání souboru externího číselníku do systému, přiřazení data platnosti a verze. | - |
| ST-SPC-002 | Nahrání individuálních úprav externího číselníku | Umožnit nahrání souboru individuálních úprav externího číselníku (od OZP). Umožnit pro speciální přístupové právo správu externích číselníku editací v uživatelské rozhraní s protokolem/seznamem o jejich realizaci včetně obsahu změn.  | - |
| ST-SPC-003 | Nahrání individuálně nasmlouvaných cen léčiv | Umožnit nahrávání individuálně nasmlouvaných cen do číselníků léčiv a léčivých prostředků s protokolem o jejich nahrání (je součástí souboru individuálních úprav OZP).  | - |
| ST-SPC-004 | Dopočítání rozdílu individuálních cen a dávek | Umožnit dopočítání rozdílu, při změně individuálních cen u doposud proplacených dávek při zpětném zavedení individuálních cen. | - |
| ST-SPC-005 | Realizace dat platnosti položek číselníku | U všech číselníků budou atributy platnost od a platnost do u každé položky a verze. | - |
| ST-SPC-006 | Nahrání předchozí verze externího číselníku | Musí být možné nahrát soubory předchozí verze (někdy jsou soubory zaslány na přeskáčku), systém s tímto musí počítat a provést správně aktualizaci položek (zejména jejich platnosti). | - |
| ST-SPC-007 | Správa interních číselníků | Umožnit standardní správu interních číselníku editací v uživatelské rozhraní. | - |
| ST-SPC-008 | Identifikace změn v souboru individuálních úprav | Při nahrání souboru individuálních úprav systém zobrazí seznam realizovaných změn (počet aktualizovaných položek). | - |
| ST-SPC-009 | Správa interních parametrů a nastavení ICIS pro možnost interních kontrol a validací | Umožnit definování a správu interních parametrů ICIS pro možnost spouštění kontrol a validací v rámci procesů jednotlivých modulů.  | - |

# Administrace (ADM)

Tato kapitola neobsahuje žádná data.

# Bezpečnost (BZP)

| Kód | Název požadavku | Detailní popis požadavku | Související proces |
| --- | --- | --- | --- |
| ST-BZP-000 | Splnění technických požadavků zákona č.181/2014 Sb., o kybernetické bezpečnosti a souvisejících vyhlášek (v součinnosti s Objednatelem) | Splnění požadavků vyhlášky č.316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) | - |
| ST-BZP-001 | Ochrana integrity komunikačních sítí  | Splnit požadavky řízení bezpečného přístupu mezi vnější a vnitřní sítí.Zavedení segmentace zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí.Používat kryptografické prostředků pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií.Zavést opatření pro odstranění nebo blokování přenášených dat, které neodpovídají požadavkům na ochranu integrity komunikační sítě. | - |
| ST-BZP-002 | Ověřování identity uživatelů | Zajistit ověřování identity uživatelů a administrátorů před zahájením jejich aktivit v informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury a významném informačním systému. | ST-AIM |
| ST-BZP-003 | Heslo | Ověřování identity uživatelů, které používá autentizaci pouze heslem, zajišťovat tak, že bude splňovat:* minimální délka hesla osm znaků,
* minimální složitost hesla tak, že heslo bude obsahovat alespoň 3 z následujících čtyř požadavků:
* nejméně jedno velké písmeno,
* nejméně jedno malé písmeno,
* nejméně jednu číslici, nebo
* 4. nejméně jeden speciální znak odlišný od požadavků uvedených v bodech 1 až 3,
* Maximální dobu pro povinnou výměnu hesla nepřesahující sto dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací.
* Zamezit opětovnému používání dříve používaných hesel a neumožní více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin.
* Provádět opětovné ověření identity po určené době nečinnosti.
* V případě, autentizaci heslem administrátora, zajistí prosazení minimální délky hesla patnáct znaků při dodržení požadavků.
 | - |
| ST-BZP-004 | Řízení přístupových oprávnění | Zajistit řízení přístupových oprávnění pro přístup k jednotlivým aplikacím a datům a pro čtení dat, pro zápis dat a pro změnu oprávnění. | ST-AIM |
| ST-BZP-005 | Ochrana před škodlivým kódem | Zajistit ochranu před škodlivým kódem, který zajistí ověření a stálou kontrolu komunikace mezi vnitřní sítí a vnější sítí, serverů a sdílených datových úložišť a pracovních stanic. | - |
| ST-BZP-006 | Logování činností | Zaznamenávat činností (logování) informačního systému, jejich uživatelů a administrátorů:Zajistit sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti.Zajistit ochranu získaných informací před neoprávněným čtením nebo změnou.Zaznamenávat:* přihlášení a odhlášení uživatelů a administrátorů,
* činnosti provedené administrátory,
* činnosti vedoucí ke změně přístupových oprávnění,
* neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
* zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému,
* automatická varovná nebo chybová hlášení technických aktiv,
* přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a
* použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

Zaznamenané záznamy činností uchovávat nejméně po dobu 3 měsíců. | - |
| ST-BZP-007 | Systémový čas | Zajistit nejméně jednou za 24 hodin synchronizaci jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému. | - |
| ST-BZP-008 | Detekce kybernetických bezpečnostních událostí | Zajistit použití nástroje pro detekci kybernetických bezpečnostních událostí, který zajistí ověření, kontrolu a případně zablokování komunikace v rámci vnitřní komunikační sítě a serverů patřících do informačního systému. | - |
| ST-BZP-009 | Aplikační bezpečnost | Zajistit provádění bezpečnostních testů zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů.Zajistit trvalou ochranu:* aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou a
* transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.
 |  |
| ST-BZP-010 | Kryptografické prostředky | Při používání kryptografické ochrany stanovit* úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu a
* pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat a
* v souladu s bezpečnostními potřebami a výsledky hodnocení rizik používat kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a průkaznou identifikaci osoby za provedené činnosti.
 |  |
| ST-BZP-011 | Zajišťování úrovně dostupnosti | Zajistit zálohování důležitých technických aktiv informačního systému:* využitím redundance v návrhu řešení a
* zajištěním náhradních technických aktiv v určeném čase.
 |  |

# Autentizace a identity management (AIM)

| Kód | Název požadavku | Detailní popis požadavku | Související proces |
| --- | --- | --- | --- |
| ST-AIM-000 |  | Systém umožní přístup jen oprávěným uživatelům pomocí SSO + přebírat oprávnění dle AD. Přístupy budou logovány a monitorovány. Řízení přístupu bude škálovatelné až na úroveň tlačítek, obrazovek. | - |
| ST-AIM-001 | Přihlášení do ICIS pomoci SSO | Umožnit přihlášení uživatele do nového ICIS pomocí SSO + přebírat oprávnění dle definovaných funkčních rolí dle AD. | - |
| ST-AIM-002 | Komunikace s externími systémy pouze pomocí komunikačního rozhraní | S externími subjekty komunikovat primárně přes Portál OZP či jiné rozhraní na základě předem definované komunikace dotaz-odpověď. Podnět pro načítání dotazů a jejich zpracování vždy vychází z ICIS. Detailně monitorovat externí komunikace na rozhraní. | - |
| ST-AIM-003 | Provázání přidělování oprávnění na personální systém | Provázat přidělování oprávnění do ICIS přes personální systém, kdy na základě zařazení nového pracovníka na danou pozici v rámci organizační struktury budou pracovníkovi automaticky přidělena příslušná oprávnění do ICIS resp. celé AD. Při změně pozice změnit automaticky i oprávnění. Pracovníci IT mohou konkrétní oprávnění pro uživatele případně dále modifikovat.  | - |
| ST-AIM-004 | Dle technologie umožnit maximální škálovatelnost oprávnění nad DB s využitím AD | Umožnit, dle možností zvolené technologie, řízení oprávnění k DB ICIS dle AD a nastavených funkčních rolí pro správa DB (zálohování apod. bez možnosti zobrazení dat) vs. vkládání či čtení dat v rozsahu konkrétních tabulek pro konkrétní skupiny uživatelů. | - |
| ST-AIM-005 | Evidování oprávnění k ICIS v co nejmenší granularitě | Aplikační role evidovat v granularitě přístupu k obrazovce, navigaci, dokumentů, tlačítek až konkrétních data (osobní, výkazy péče, ekonomické přehledy, eko. deníky). | - |
| ST-AIM-006 | Zohlednění příslušnosti k pobočce v rámci definic oprávnění  | Umožnit nastavení oprávnění v agendách ekonomických (platby zaměstnavatelů apod.) dle poboček, registrové data o pojištěnci (osobní, platební povinnosti apod.) bez omezení na pobočku. | - |
| ST-AIM-007 | Kontrola na neslučitelná oprávnění pro jednoho uživatele | Kontrolovat neslučitelnost oprávnění – jestliže v rámci jednoho procesu může uživatel provést všechny kroky (má všechna oprávnění), upozornit uživatele při přidělování oprávnění (byly nastaveny dvě funkční role, které obsahují všechny aplikační daného procesu apod.). | - |
| ST-AIM-008 | Delegování profilů mezi uživateli | Umožnit delegování profilů na definovaný časový interval – uživatel sám může delegovat jinému uživateli (poslat v tu chvíli notifikaci správci) nebo administrátor může nastavit komukoli. | - |

# Pořizovací programy (POP)

| Kód | Název požadavku | Detailní popis požadavku | Související proces |
| --- | --- | --- | --- |
| ST-POP-000 |  | Systém bude umožňovat přímé pořízení dat z papírových podkladů bez nutnosti využívání aplikací třetích stran a následné transformaci dat. | - |
| ST-POP-001 | Pořizování dávek v elektronické i papírové podobě přímo do ICIS | Umožnit pořizování dávek v papírové i elektronické podobě přímo do ICIS. Co nejvíce  sjednotit průchod papírových i elektronických kdávek a provádět kontroly při pořizování jen za účelem upozornění na možné překlepy.  | - |
| ST-POP-002 | Načítání dat externě vytěžovaných | Umožnit načítání aktuálně definovaných datových struktur dle OZP pro PPPZ, HOZ a přehledů OSVČ, které vytěžují (pořizují) externí firmy. V ICIS mít pak přístup jak k datům tak naskenovaným předlohám, ze kterých byla data pořizována. | - |
| ST-POP-003 | Vyhledávání a zobrazování naskenovaných receptů při revizích vykázané péče | Umožnit interně evidovat skeny receptů s možností rychlého dohledání jejich obrazů přímo z ICIS pomocí metadat, při revizích dokladů.  | - |

# Systém varování (SVA)

Tato kapitola neobsahuje žádná data.