Příloha č. 2

**Minimální technické požadavky Komplexní softwarová podpora klinické farmacie**

VZ-2024-000096

Zkratky

AD Active directory – správa uživatelských nastavení

API aplikace

ČLSJEP Česká lékařská společnost Jana Evangelisty Purkyně

ČOSKF Česká odborná společnost klinické farmacie

FTD farmakoterapeutického doporučení

HW hardware

KLK seznam léčivých přípravků registrovaných v ČR, pro něž byl schválen specifický léčebný program, potravin pro zvláštní lékařské účely a pomocné číselníky

LDAP protokol pro ukládání a přístup k datům na adresářovém serveru (Lightweight Directory Access Protocol)

MS Microsoft

NIS nemocniční informační systém zadavatele

PC osobní počítač

SCAU Seznam cen a úhrad (léčivých přípravků a potravin)

SÚKL Státní ústav pro kontrolu léčiv

SW software

1. Popis stávajícího stavu

Zadavatel má v rámci rozvoje a profesionalizace jednotlivých činností zájem realizovat projekt komplexní softwarové podpory pro práci klinických farmaceutů. V rámci tohoto projektu požaduje implementovat tržně dostupný moderní software pro klinickou farmacii, který má splňovat dále uvedené požadavky.

1. Základní vlastnosti požadovaného softwaru

Zadavatel požaduje následující základní technické vlastnosti:

* moderní software s uživatelským rozhraním webové aplikace;
* multiplatformní řešení (Databázově plně nezávislý, podpora všech serverových platforem);
* responzivní design uživatelského rozhraní softwaru, a to včetně možnosti portace uživatelského rozhraní i na mobilní zařízení;
* integraci na nemocniční informační systémy zadavatele pomocí API či pomocí integrační platformy:
  + přenos pacientských dat z databáze NIS (bude řešeno v úvodní analýze)
  + synchronizace pracovišť zadavatele (kliniky, oddělení)
  + integrace minimálně následujících číselníků:
    - Číselník léčiv (SCAU, KLK)
    - Číselník klinik
    - Číselník oddělení
    - Číselník diagnóz
    - Číselník externích zdravotnických zařízení
    - Číselník zaměstnanců
    - Číselník plátců zdravotní péče (pojišťoven)
  + přenos zdravotních výkonů klinické farmacie do účetního systému zadavatele
  + přenos pacientských žádanek vztahujících se ke klinické farmacii
  + předávání hlášení o nežádoucích účincích léčiv SÚKL
* plná podpora aktuálních zákonných norem a předpisů
* elektronická evidence úkonů klinického farmaceuta v návaznosti na standardní postupy ČOSKF, ČLS JEP ([metodika\_1.pdf (coskf.cz)](http://www.coskf.cz/media/files/metodika_1.pdf))
* integrace na Active directory Microsoft/Kerberos (včetně SSO)
* tvorba podkladů pro vykazování výkonů nejen zdravotním pojišťovnám, datová integrace na SW zadavatele pro vykazování.

1. Funkční vlastnosti požadovaného softwaru

Zadavatel požaduje, aby SW měl následující funkční vlastnosti:

* přehled klinik a oddělení zadavatele, aktualizovaný a synchronizovaný s datovými zdroji zadavatele. U klinik/oddělení, aby zobrazoval počet nově hospitalizovaných pacientů;
* přehled pacientů na klinice a oddělení, aktualizovaný a synchronizovaný s datovými zdroji zadavatele. U každého pacienta v seznamu zobrazovat základní údaje (minimálně rodné číslo, věk, délku hospitalizace, ošetřujícího lékaře). Umožňovat filtrovat seznam dle tříd rizikovosti a dle již provedených úkonů;
* aktualizaci pacientských dat z NIS v pravidelných intervalech, včetně užívaných léků;
* umožňovat rozdělení pacientů na hospitalizované, ambulantní a externí (pacienti klinické farmacie, kteří neprojdou evidencí přes NIS);
* umožňovat zaevidovat vlastního externího pacienta bez nutnosti zásahu do NIS;
* vykazování všech typů výkonů vztahujících se ke klinické farmacii dle vyhlášky č. 243/2021 Sb. a č. 482/2021 Sb.;
* hlídání limitů frekvence vykazování výkonů;
* vstupní kontrolu včetně úvodního stanovení rizikovosti pacienta, záznam lékové anamnézy, výběr užívaných léků z číselníků;
* tvorbu a editaci farmakologického plánu (v okně kromě textů plánu zobrazit i detaily pacienta, výsledky vstupní kontroly pacienta, navázané výkony) s možností uložení předdefinovaných textů;
* tvorbu a editaci farmakoterapeutického doporučení a odlišné verze farmakoterapeutického doporučení do propouštěcí zprávy a jejich přenos do NIS;
* stanovení podrobnějších doporučení pro jednotlivá léčiva a jejich evidence v rámci FTD. Jednotlivá léčiva vybírat z číselníku, doporučení evidovat ve strukturované formě minimálně v rozsahu metodiky ČOSKF;
* prohlížení historie péčí včetně logu všech změn v datech pacienta;
* umožňovat přidělovat pacientům příznaky, které si definuje uživatel SW;
* podpora pro statistiky a reporty v tisknutelné (.pdf) i datově zpracovatelné podobě (.xlsx, apod.)
  + možnost generování ročního výkazu pro ÚZIS
  + možnost generování reportu výkonů za určité časové období
  + možnost generování reportu pro výpis počtu pacientů s jednotlivými rizikovostmi
  + možnost generování reportů členěných dle užívaných léků, diagnóz, rizikových faktorů vstupní kontroly
  + možnost rozšíření o nové reporty na žádost zadavatele
* možnost reakce na jednotlivé typy žádanek
* možnost nahlášení nežádoucích účinků léčiv na SÚKL

1. HW a systémové požadavky

Zadavatel požaduje provoz na stávajících zařízeních s minimální konfigurací:

* virtualizované prostředí ve vlastnictví zadavatele. Nároky na HW nesmí překročit následující parametry:
* max 1 x aplikační server (6 x CPU 24 GB paměti, diskový prostor 200 GB)
* max 1 x databázový server (6xCPU, 32 GB RAM, 500 GB HDD, standardní SQL databáze (MS SQL 2022, PostgreSQL, MySQL, Maria DB apod.)).
* v případě, že řešení bude pro provoz vyžadovat licenci OS Windows 2022 a MSSQL 2022 pak je v tomto případě možné využít licence zadavatele.

Implementační služby budou fakturovány po jejich dodání na základě akceptačního protokolu, který potvrdí kompletní dodání SW a implementačních služeb do provozního prostředí zadavatele.

1. Podklady pro kalkulaci nákladů

Zadavatel požaduje, aby součástí celkové nabídkové ceny bylo:

* všechny nezbytně potřebné licence pro provoz IS včetně neomezených uživatelských licencí (multilicence);
* servisní podpora dle SLA na dobu 48 měsíců (smlouva bude uzavřena na dobu neurčitou);
* prodloužená splatnost faktur 60 dnů.

1. Další požadavky

Nabízený SW:

* musí splňovat požadavky GDPR a Zákona o kybernetické bezpečnosti uvedené v textu návrhu

smlouvy;

* integrační vazby dle výše uvedeného bodu 2. Základní vlastnosti požadovaného softwaru;
* integraci bude řešit úvodní analýza.

Zadavatel ještě před podepsáním smluv vyzve vítězného uchazeče k okamžitému (nejpozději však do 14 dnů) provedení prezentace nabízeného SW za účelem prokázání splnění **všech** požadovaných funkcionalit dle této Přílohy č.2 zadávací dokumentace.

Součástí dodávky bude dodání dokumentace – uživatelského a administrátorského manuálu v elektronickém formátu a jejich aktualizace s každou nově nasazenou verzí nebo updatem, které přinesou změny v ovládání aplikace.

Uchazeč, jako poskytovatel, bude mít povinnost informovat určené pracovníky zadavatele o nasazení/změně aktuální verze systému.

1. Požadavky na webové aplikace

Zadavatel požaduje, aby uchazečem nabízené webové aplikace obsahovaly řešení potlačující rizika dle doporučení OWASP z roku 2017 min. v rozsahu T10 (A1-A10):

**A1 – injektování -** ke zranitelnostem injektováním, např. injektováním SQL, OS a LDAP, dochází,

když se jako součást příkazu nebo dotazu odesílají do interpretu nedůvěryhodná data.

Útočníkova nepřátelská data mohou lstí přimět interpret k provedení nezamýšlených příkazů

nebo k umožnění přístupu k datům bez řádné autorizace.

**A2 – Chybná autentizace a správa relace -** funkce aplikací, které se vztahují k ověřování a správě

relace, často nejsou provedeny správně, což útočníkům umožňuje kompromitovat hesla, klíče

nebo tokeny relací anebo zneužít jiné slabiny v implementaci k tomu, aby převzali identitu

jiných uživatelů.

**A3 – Expozice citlivých dat -** mnoho webových aplikací a rozhraní API nechrání náležitě citlivá data,

jakými jsou např. finanční, zdravotní a PII. Tato slabě chráněná data útočníci mohou krást či

modifikovat, aby mohli provádět podvody s kreditními kartami, krádeže identity nebo jiné

trestné činy. Citlivá data si zaslouží zvláštní ochranu, např. šifrování dat v klidu nebo v

na cestě, stejně tak i zvláštní bezpečnostní opatření pro data v prohlížeči.

**A4 – XML externí subjekty (XXE) -** mnoho starších nebo špatně nakonfigurovaných procesorů

XML vyhodnocuje odkazy na externí entity v rámci XML dokumentů. Externí entity lze použít k

odhalení interních souborů pomocí obslužné rutiny identifikátoru URI souboru, interní sdílení

souborů, interní skenování portů, vzdálené spuštění kódu a útoky odmítnutí služby.

**A5 – Nedostatečné řízení přístupů -** omezení toho, co mají povoleno ověřovaní uživatelé, často

nejsou řádně vynucována. Útočníci mohou tyto nedostatky využít k přístupu k neoprávněným

funkcím a / nebo datům, jako je přístup k účtům jiných uživatelů, prohlížení citlivých souborů,

úprava dat ostatních uživatelů, změna přístupových práv atd.

**A6 – Ne-zabezpečená konfigurace -** dobré zabezpečení vyžaduje mít definováno a nasazeno

bezpečné nastavení aplikace, frameworků, aplikačního serveru, webového serveru, databázového serveru, platformy, cloudového úložiště, záhlaví HTTP a podrobných chybových zpráv obsahujících citlivé informace. Bezpečnostní nastavení by měla být definována, prováděna a udržována, protože výchozí hodnoty jsou často riskantní. Všechny operační systémy, rámce,

knihovny a aplikace musí být bezpečně nakonfigurovány a včas opraveny a upgradovány.

**A7 – Cross-Site Scripting (XSS**) - chyby typu XSS nastávají tehdy, když aplikace přijme

nedůvěryhodná data a odešle je webovému prohlížeči bez řádného ověření nebo escapování.

XSS útočníkům umožňuje spouštět skripty v prohlížeči oběti, které mohou unést uživatelské

relace, přetvořit webové stránky nebo přesměrovat uživatele na škodlivé stránky.

**A8 – Nezabezpečená deserializace -** často vede ke vzdálenému spuštění kódu. I když nedostatky

deserializace nemají za následek vzdálené spuštění kódu, mohou být použity k provádění útoků,

včetně jejich opakování, injekčních útoků a útoků na eskalaci privilegií.

**A9 – Použití známých zranitelných komponent -** komponenty, např. knihovny, frameworky a další

softwarové moduly, téměř vždy běží s nejvyššími oprávněními. Jestliže je zranitelná

komponenta zneužita, útok může usnadnit závažnou ztrátu dat nebo ovládnutí serveru. Aplikace

používající komponenty se známými zranitelnostmi mohou zmařit ochranu aplikací a umožnit

řadu útoků a dopadů.

**A10 – Nedostatečné protokolování a monitorování -** spojené s chybějící nebo neúčinnou odezvou

na incident, umožňuje útočníkům další vytrvalé útoky, rozšiřovat na více systémů, manipulovat,

extrahovat nebo zničit data. Většina studií porušení ukazuje, že jsou obvykle detekovány

externími stranami, nikoli interními procesy nebo monitorováním.

1. Požadavky na provedení implementace

Implementace bude zahrnovat poskytnutí veškerých potřebných licencí (včetně licencí tzv. třetích stran, neomezených uživatelských licencí (multilicence)) k řádnému užívání dodaného SW zadavatelem, které jsou již zahrnuty v ceně nabídky.

Implementace bude zahrnovat integraci dle výše uvedeného bodu č. 2. této přílohy (bude předmětem úvodní analýzy).

Zadavatel požaduje provedení plné implementace řešení takovým způsobem, aby výsledkem implementace byly dodavatelem splněny následující body:

* vytvoření úvodní analýzy popisující detailně cílové řešení. Na základě této analýzy bude provedena implementace SW. Dokument s procesní analýzou slouží zejména ke vzájemnému pochopení a vyjasnění všech aktivit, kterých se následná implementace SW dotkne. Výstupem bude dokument „Implementační analýza“, který projde schvalovacím procesem zadavatele.
* návrh infrastruktury pro provoz SW v podmínkách zadavatele (součást úvodní analýzy);
* provedení komplexní integrace na systémy a jiné datové zdroje zadavatele provozované v prostředí zadavatele a nutné k integraci daného řešení;
* integrace datových zdrojů (databáze pacientů, číselníky apod.);
* instalace a provozní optimalizace;
* příprava pro MS AD, LDAP;
* vytvoření testovacího prostředí o přiměřené konfiguraci;
* řádné otestování všech instalovaných součástí nabízeného SW v testovacím prostředí a následně i v ostrém provozu;
* školení správců IS v takovém rozsahu, aby byli schopni řešit funkčnost systému v rámci FNOL, byli schopni poskytovat uživatelskou podporu pracovištím zadavatele, spravovat systém po stránce nastavování jednotlivých funkcionalit, nastavování přístupových oprávnění, uměli poskytovat podporu klíčovým uživatelům, uměli popsat požadavky jednotlivých pracovišť směrem k poskytovateli služby…;
* školení klíčových uživatelů jednotlivých pracovišť zadavatele v rámci, kterého si osvojí všechny úkony spojené s použitím základních funkcí SW, aby uměli poskytovat podporu uživatelům, uměli popsat požadavky pracoviště směrem k administrátorovi systému… a to formou teoretické průpravy i praktického zaškolení na takové úrovni, aby byli schopni školit další uživatele SW na svých pracovištích ve FNOL;
* u všech školení dodání zápisu s jmenovitým seznamem proškolených osob a obsahem školení;
* předání kompletní dokumentace (uživatelské, vývojářské, technické a bezpečnostní), dále architektonický model pro konkrétní implementaci a zdrojové kódy implementovaného SW s každou dodanou aktualizací;
* předání uživatelského a administrátorského manuálu v elektronické podobě v českém jazyce;
* ověření, zda poskytované webové aplikace splňují řešení potlačující rizika v oblasti bezpečnosti webových aplikací dle doporučení OWASP z roku 2017 (viz Příloha č.6) min. v rozsahu T10 (A1-A10);
* aktivní dohled a podpora při startu a v průběhu zkušebního provozu, popřípadě na výzvu zadavatele provést úkony v rozsahu dle potřeby, ale min. v délce jednoho měsíce;
* rozběh ostrého provozu.

O provedené implementaci a jejím splnění bude sepsán akceptační protokol, který bude obsahovat popis případných nedostatků. Implementace bude považována za dokončenou až v okamžiku, kdy bude SW řádně bez závad a nedodělků (bez výhrad) fungovat v ostrém provozu a bude oběma stranami akceptována podpisem protokolu o provedení implementace.

Poskytovatel zahájí plnění předmětu zakázky do 7 pracovních dnů po oboustranném podpisu smlouvy (analýza) a implementuje IS v **plné** míře výše uvedených požadavků a funkcionalit nejpozději do 7 měsíců od zahájení plnění dle následujícího harmonogramu:

|  |  |  |  |
| --- | --- | --- | --- |
| **Činnost** | **Od** | **Do** | **Pozn.:** |
| Podpis smlouvy | T = datum podpisu smlouvy  M = měsíc | | |
| Úvodní analýza |  | T + 2 M |  |
| Implementace, konfigurace, customizace, školení (testovací prostředí) |  | T + 4 M |  |
| Implementace, konfigurace, customizace, školení (produkční prostředí) |  | T + 6 M |  |
| Testovací provoz (běží paralelně s Implementací, konfigurací a customizací) |  | T + 6 M |  |
| Ověřovací provoz |  | T + 7 M |  |
| **Rutinní provoz** | **T + 7 M** |  |  |

1. Servisní podpora

Požadavky na servisní podporu jsou popsány v Příloze č. 4 – Návrh Smlouvy o poskytování licencí, služeb a technické podpory a v SLA jako její příloha č.2.