Příloha č. 2

**Minimální technické požadavky na informační systém pro sběr a analýzu dat pro odhad radiační zátěže pacientů.**

**Zkratky:**

FNOL Fakultní nemocnice Olomouc

GDPR Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)

HW hardware

IS informační systém pro sběr a analýzu dat pro odhad radiační zátěže pacientů

SLA úroveň dohodnutých služeb (service level agreement)

SW software

ÚRO Ústav radiačnej ochrany, s.r.o. ([www.uro.sk](http://www.uro.sk))

VZMR veřejná zakázka malého rozsahu

1. **Popis aktuálního stavu**

Zadavatel provozuje pro sběr a analýzu dat pro odhad radiační zátěže pacientů informační systém UROKLIN (automatizovaný systém DQC - Dose Quality Control) poskytovaný firmou ÚRO. Anonymizovaná data zpracovává ÚRO a výstupy poskytuje zadavateli. Zadavatel nově požaduje zpracování dat ve své počítačové síti.

1. **Předmět plnění**

Předmětem VZMR je poskytování služeb stávajícího IS nebo jeho náhrady dle požadavků této Přílohy. Poskytované služby se budou řídit dle jednotlivých SLA uvedených v návrhu servisní smlouvy jako její Příloha č. 1 – SLA.

1. **Podklady pro kalkulaci nákladů**

 Zadavatel požaduje, aby součástí nabídkové ceny:

* byly všechny potřebné licence, HW a SW pro bezproblémový chod a využívání IS zadavatelem včetně neomezených uživatelských licencí. To se týká i eventuelně potřebných licencí pro provozování klienta (např. Java);
* byla servisní podpora dle SLA na dobu 48 měsíců pro 55 připojených zařízení (smlouva bude podepsána na dobu neurčitou);
* byla prodloužená splatnost faktur 60 dnů.
1. **Požadavky na funkcionality IS**

IS při předání k užívání zadavateli musí:

* umět provádět záznam kvantitativních dat o ozáření pacientů pro min. následující modality (za předpokladu, že tyto systémy informaci o ozáření pacienta poskytují):
* stacionární a modilní skiagrafie a skiaskopie
* mammografie
* CT
* zubní rtg
* angiolinky
* planární scintigrafie
* SPECT
* SPECT/CT
* PET
* PET/CT
* cone-beam CT;
* umět zpracovat kvantitativní informaci o ozáření pacientů na základě informací z DICOM hlaviček a/nebo strukturovaných reportů a/nebo obrazových dávkových reportů pomocí technologie OCR a/nebo MPPS informací;
* mít přímé napojení jednotlivých modalit (prostřednictvím strukturovaných dávkových reportů nebo přímou analýzou zaslaných obrazů/řezů) a rovněž musí umět zpracovat data zaslaná z nemocničního PACS systému;
* umět ukládat data v databázové podobě a umožňovat vyhledávání konkrétních pacientských záznamů s pomocí rodného čísla pacienta a/nebo jména pacienta;
* umět zaznamenávat veškeré informace důležité pro odhad radiační zátěže a jejich seznam musí být modifikovatelný pro daný přístroj. Parametry musí být identifikovány na základě DICOM tagu;
* umět zaznamenávat veškeré informace z následujícího množství a typů radiologických přístrojů (seznam platný ke konci 02/2022) a umožňovat snadné rozšíření o další přístroje:



* umět nastavit signální hodnoty překročení lokálních a národních diagnostických referenčních úrovní;
* umět u každého pacienta přehledně zobrazit všechna ve FNOL absolvovaná vyšetření včetně příslušných dávkových parametrů;
* umět provádět souhrnné výpisy všech záznamů z dané modality za libovolné časové období a exportovat je min. do formátu .csv.
1. **Technické požadavky na IS**

Zadavatel požaduje provoz IS v jeho počítačové síti, tzn. veškeré potřebné licence, SW a HW prostředky, dodá a zprovozní poskytovatel. Všechny finanční náklady již bude zahrnovat jednotková cena za připojené modality.

**Min. technické požadavky na konfiguraci poskytnutého** **serveru**:

* rackové provedení (z důvodu umístění do serverovny zadavatele), velikost max. 2U (z důvodu umístění do serverovny zadavatele), vzdálený management: možnost vzdáleného ovládání serveru na úrovni HW, odpovídající IMM with remote presence, iLO Advanced apod. (trvalá licence s plnou funkcionalitou) včetně podpory KVM a mapování ISO instalačních médii, LAN min. 2x 1Gbps, systémový disk min. kapacita 240 GB v RAID 1, datový disk min. kapacita 8TB v RAID1;
* operační systém musí podporovat zálohovací SW IBM Spectrum Protect ve verzi 8.1.13 a vyšší;
* poskytovatel zajistí veškerou potřebnou certifikaci pro WAN přístup k serveru.

Při předání IS poskytovatelem k užívání zadavateli musí IS:

* mít dvoufaktorové ověření při přihlašování uživatelů (login, heslo, sms);
* umět průběžně monitorovat provoz všech připojených modalit a zobrazovat hodnoty základních monitorovaných veličin;
* umožňovat přístup k aplikaci a datům odkudkoliv přes webový přístup (**webová aplikace**);
* umožňovat přístup k aplikaci přes webový prohlížeč min.:
* MS Edge chromium 70 a novější;
* Google Chrome 70 a novější;
* Mozilla Firefox 70 a novější;
* Opera 60 a novější;
* Safari 10 a novější.

a služba byla provozovatelná s garancí poskytovatele na aktualizace aplikace pro nové verze webových prohlížečů;

* splňovat všechny požadavky dle bodu **7. Požadavky na webové aplikace;**
* umět nastavení práv přístupů určených uživatelů min. pro úroveň:
* superadministrátor (předpokládá se pro zaměstnance poskytovatele);
* administrátor (k nastavování lokálních diagnostických referenčních úrovní; předpokládá se pro určené zaměstnance zadavatele);
* standardní uživatel (prohlížení záznamů, vytváření výpisů).
* být kompletně v české lokalizaci, tedy nejen v českém, případně slovenském jazyce ale i v české legislativě;
* umět využívat doposud vytvořenou databázi údajů od stávajícího poskytovatele služeb Ústavu radiačnej ochrany, s.r.o., Staničná 1062/24, SK - 911 05 Trenčín | Slovakia produkt DQC monitor;
* ověřoval uživatele buďto dvou faktorovým způsobem nebo v MS Active Directory zadavatele (ADFS a SSO);
* archivoval logování spuštění a průběhů aplikace a online přístup administrátorů zadavatele k logům min. po dobu 18 měsíců. Logy musí obsahovat informace min. o činnostech:
* přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů;
* provedených administrátory;
* úspěšné i neúspěšné manipulace s účty, oprávněními a právy;
* uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému;
1. **Další požadavky**

 Uchazeč musí být poskytovatelem/výrobcem nebo mít od něj souhlas k přístupu a změnám zdrojových kódů,

 datových struktur nabízeného IS a služby tak, aby mohl provádět úpravy dle požadavků zadavatele (tuto

 skutečnost doloží uchazeč potvrzením od poskytovatele / výrobce);

 Nabízený IS:

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

 smlouvy o poskytování služeb, technické podpory a servisu;

 Zadavatel v případě náhrady IS, ještě před podepsáním smlouvy, vyzve vítězného uchazeče k okamžitému

 (nejpozději však do 14 dnů) provedení **prezentace** nabízeného IS za účelem prokázání splnění **všech**

 požadovaných funkcionalit dle této Přílohy č.2 zadávací dokumentace.

 Součástí poskytovaných služeb bude poskytnutí uživatelského a administrátorského **manuálu** v běžně

 dostupném elektronickém formátu (např. Word, Excel, PDF) a jejich aktualizace s každou nově nasazenou

 verzí, která přinese změny v ovládání aplikace. Uchazeč, jako poskytovatel, bude mít povinnost informovat

 určené pracovníky zadavatele o nasazení/změně aktuální verze systému.

Zadavatel požaduje **zaškolení** česky/slovensky mluvícím specialistou min.:

* 1 pracovníka zadavatele na úrovni role administrátora,
* 2 pracovníky zadavatele na úrovni uživatele aplikace

 Zadavatel požaduje pro nahlášení požadavků a závad, a pro konzultace, poskytnutí **Hotline** poskytovatele.

 Zadavatel požaduje **vedení evidence** svých požadavků a hlášení závad poskytovatelem v elektronické podobě.

Zadavatel pro správu a řešení jeho požadavků poskytne poskytovateli **vzdálený přístup** do IS dle pravidel uvedených ve Smlouvě jako její Příloha č. 4 – Ujednání o poskytnutí vzdáleného přístupu.

1. **Požadavky na webové aplikace**

 Zadavatel požaduje, aby uchazečem nabízené webové aplikace obsahovaly řešení potlačující rizika

 dle doporučení OWASP z roku 2017 (viz Příloha č.6) 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, SW a HW prostředků k dodanému

 IS, které jsou již zahrnuty v ceně nabídky.

 **V případě náhrady IS**:

 zadavatel požaduje provedení implementace takovým způsobem, aby výsledkem implementace byly

 poskytovatelem služby splněny následující body:

* vytvoření úvodní analýzy popisující detailně cílové řešení. Na základě této analýzy bude provedena implementace/nasazení IS. Dokument s procesní analýzou slouží zejména ke vzájemnému pochopení a vyjasnění všech aktivit, kterých se následná implementace IS dotkne. Výstupem bude dokument „Implementační analýza“, který projde schvalovacím procesem zadavatele;
* migrace dat od stávajícího poskytovatele služeb Ústavu radiačnej ochrany, s.r.o., Staničná 1062/24, SK - 911 05 Trenčín | Slovakia produkt DQC monitor;
* řádné otestování všech instalovaných součástí nabízeného IS 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 IS 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 zadavatele, v rámci kterého si osvojí všechny úkony spojené s použitím základních funkcí IS, 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 IS zadavatele;
* u všech školení dodání zápisu s jmenovitým seznamem proškolených osob a obsahem školení;
* předání uživatelského a administrátorského manuálu v elektronické podobě v českém/slovenském 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 v průběhu testování, popřípadě na výzvu zadavatele provést úkony v rozsahu dle potřeby, ale min. v délce jednoho měsíce;
* rozběh ostrého provozu.

**V případě implementace stávajícího IS v počítačové síti zadavatele:**

zadavatel požaduje provedení implementace takovým způsobem, aby výsledkem implementace byly poskytovatelem služby splněny následující body:

* vytvoření popisu cílového řešení provozu služby v počítačové síti zadavatele. Na základě tohoto popisu bude provedena implementace/nasazení IS. Dokument s procesní analýzou slouží zejména ke vzájemnému pochopení a vyjasnění všech aktivit, kterých se následná implementace IS dotkne.
* řádné otestování všech instalovaných součástí nabízeného IS 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 IS po stránce nastavování jednotlivých funkcionalit, nastavování přístupových oprávnění, uměli poskytovat podporu klíčovým uživatelům, uměli popsat požadavky jednotlivých pracovišť směrem k poskytovateli služby…;
* předání uživatelského a administrátorského manuálu v elektronické podobě v českém/slovenském 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 v průběhu testování, 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 IS řádně bez závad a nedodělků 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 3 měsíců od zahájení plnění.

1. **Servisní podpora**

Servisní podpora bude součástí poskytovaných služeb a paušálu. Požadavky jsou popsány v Příloze č. 4 – Návrh Smlouvy o poskytování služeb technické podpory a servisu, včetně její Přílohy č. 2 – Podrobný popis služeb (SLA).