Příloha č. 2

**Minimální technické požadavky**

**Zkratky:**

DTMF tónová telefonní volba (Dual-tone multi-frequency)

FNOL Fakultní nemocnice Olomouc

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

HSS hromadný svolávací systém

ICT informační a komunikační technologie (information and communication technologies)

MS Microsoft

NB přenosný osobní počítač (notebook, laptop)

OSWAPS (Open Web Application Security Project) - projekt a komunita zabývající se bezpečností webových aplikací

PC osobní počítač (personal computer)

SLA úroveň dohodnutých služeb (service level agreement)

**1. Popis stávajícího stavu**

FNOL provozuje sofistikovaný svolávací systém pro aktivaci traumaplánu. Systém je úzce vázán na konkrétní ICT zařízení.

Účelem dále uvedených minimálních technických požadavků na poskytování služeb pro provoz svolávacího systému pro Fakultní nemocnici Olomouc je realizování rozšíření jeho funkcionalit a využití i pro další aktivity, než jen svolávání při aktivaci traumaplánu. Minimální technické požadavky byly stanoveny na základě marketingového průzkumu.

**2. Předpoklad**

Zadavatel pro provoz hromadného svolávacího systému předpokládá:

* cca 1000 aktivních účastníků ve všech scénářích s možností rozšíření až na cca 4 500 (všichni zaměstnanci zadavatele);
* min 50 souběžných hovorů;
* *vyrozumění formou:*
* *SMS – cca 210 SMS za 1 měsíc – využití SMS brány poskytovatele HSS (u SMS je u zobrazení odesílatele místo telefonního čísla požadován alias „FN Olomouc“);*
* *hlasem - cca 480 telefonních hovorů za 1 měsíc – využití služby poskytovatele HSS;*
* *e-mailem;*
* využití emailového serveru poskytovatele;
* neomezený počet scénářů;
* servisní podporu na dobu neurčitou dle SLA;
* prodloužená splatnost faktur 60 dnů.

**3. Požadavky na hromadný svolávací systém.**

Zadavatel požaduje:

* otevřený svolávací systém – customizace na míru požadavkům zadavatele;
* uchazeč musí být poskytovatelem/výrobcem nebo mít od něj souhlas k přístupu a změnám zdrojových kódů, datových struktur tak, aby mohl provádět úpravy dle požadavků zadavatele (tuto skutečnost doloží uchazeč potvrzením od poskytovatele / výrobce);
* využití min. pro svolávání traumaplánu, krizového štábu, operativních porad, operativního hlasování…;
* možnost nastavení práv až na úroveň jednotlivých typů a skupin svolávání (tzv. scénářů);
* možnost operativního hlasování odpovědí klávesou z telefonu pomocí DTMF;
* aby systém byl provozován **v cloudovém prostředí poskytovatele** služby;
* webové řešení pro více subjektů;
* možnost spustit svolávání z libovolného zařízení (PC, tablet, mobil, NB…);
* 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.
* aby služba byla provozovatelná s garancí poskytovatele na aktualizace aplikace pro nové verze webových prohlížečů;
* nastavení práv přístupů určených uživatelů aplikace min. pro úroveň:
* superadministrace pro celou aplikaci;
* administrace jednotlivých scénářů;
* svolávání vybraných scénářů;
* prohlížení vybraných scénářů.
* ověření uživatele v active directory;
* archivaci 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;
* neprovedení činností v důsledku nedostatku přístupových práv a oprávnění;
* uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému;
* celou aplikaci v české lokalizaci, tedy nejen v českém jazyce ale i v české legislativě;
* **převod** online napsaného libovolného **textu do hlasu** – **česká lokalizace** a odeslání účastníkům daného scénáře;
* možnost tvorby vlastních vícenásobných svolávacích scénářů (skupin uživatelů), min. dvouúrovňových, tj. možnost z jednoho scénáře volat/spouštět další samostatné scénáře;
* možnost před spuštěním daného scénáře upravit seznam předdefinovaných svolávaných účastníků. Prvotní nastavení seznamu bude provedeno při tvorbě scénáře, další upřesnění bude umožněno před spuštěním scénáře jejich zaškrtnutím nebo odškrtnutím;
* možnost tvorby vlastních předdefinovaných textů vlastními zaměstnanci zadavatele pro svolávání jednotlivých scénářů;
* možnost tvorby předdefinovaných hlasových nahrávek pro jednotlivé svolávané scénáře v běžně dostupném formátu (.mp3, .ogg apod.);
* automatické zveřejnění textu mimořádné události na televizích v čekárnách zadavatele přes aplikaci Ki-Wi Digital (Ki-Wi Digital s.r.o., IČ 27816451, [www.ki-wi.cz](http://www.ki-wi.cz)), kterou již zadavatel využívá. Zadání textu musí být s možností spouštění v rámci scénáře nebo samostatně.
* zpětné potvrzení svolávaného účastníka scénáře tlačítkem na mobilu z výběru předem definovaných možností;
* automatické zpětné potvrzení o předání odeslané informace do **online** přehledu o průběhu svolávání;
* možnost nastavení počtu opakování pro případ, že svolávaný nereagoval nebo byl nedostupný nebo obsazen;
* možnost aktivace účastníka scénáře na min. 2 telefonních číslech;
* **online** přehled o průběhu svolávání na jednotlivých telefonních číslech, podrobné informace o stavu volání: nezvedá / obsazeno / neexistující číslo / zvolená odpověď;
* automatický report událostí (číselný, množstevní, grafický …);
* kompletní historii průběhu události – datum a čas, uživatel, výsledky atd. min. po dobu 18 měsíců s možností odmazávání pouze starších záznamů administrátorem systému nebo automaticky dle nastaveného parametru;
* tisk výsledků – libovolného protokolu administrátorem zadavatele z archivu se všemi náležitostmi pro archivaci (min. za posledních 18 měsíců).;

**4. Další požadavky**

Nabízený svolávací systém musí:

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

Smlouvy;

- umožňovat napojení na MS Active Directory zadavatele, telefonní seznamy zadavatele,

případně další informační systémy třetích stran provozovaných u zadavatele prostřednictvím

datových standardů, kde klíčovým slovem bude osobní číslo zaměstnance zadavatele.

Případnou integraci bude řešit úvodní analýza. Uchazeč se zavazuje poskytnout součinnost při

této integraci.

- služba bude poskytována na HW prostředcích uchazeče, případně jeho smluvního partnera.

Datové úložiště a servery pro požadovanou službu musí být umístěny na území České

republiky. Informace uvede uchazeč v Příloha č.5 – Čestné prohlášení.

* zadavatel požaduje doložit úroveň bezpečnosti poskytovaných cloudových služeb alespoň jedním aktuálně platným z těchto dokumentů/certifikátů:
* ČSN ISO/IEC 27001;
* Auditní zprávu SOC 2 Type II (AT101);
* ISO 27017.

Zadavatel požaduje šifrovanou komunikaci (TLS/VPN) přes internet.

Součástí dodávky bude dodání dokumentace – uživatelského a administrátorského manuálu v elektronickém formátu 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 svolávacího systému.

**5. 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.

**6. Požadavky na provedení implementace**

Implementace bude zahrnovat poskytnutí veškerých potřebných licencí k dodanému svolávacímu systému, které jsou již zahrnuty v ceně nabídky.

Implementace bude zahrnovat migraci (import) stávajících potřebných dat, bude předmětem úvodní analýzy.

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 svolávacího systému. Dokument s procesní analýzou slouží zejména ke vzájemnému pochopení a vyjasnění všech aktivit, kterých se následná implementace svolávacího systému dotkne. Výstupem bude dokument „Implementační analýza“, který projde schvalovacím procesem zadavatele.
* provedení komplexní integrace na systémy a jiné datové zdroje zadavatele (viz. integrační vazby) provozované v prostředí zadavatele a nutné k integraci daného řešení;
* řádné otestování všech instalovaných součástí nabízeného svolávacího systému v testovacím prostředí a následně i v ostrém provozu;
* školení správců HSS v takovém rozsahu, aby byli schopni řešit funkčnost systému v rámci FNOL, byli schopni poskytovat uživatelskou podporu pracovištím zadavatele, zvládli databázové struktury dodávaného svolávacího systému a byli schopni vytvářet reporty a grafické výstupy dat;
* školení administrátorů systému v takovém rozsahu, aby byli schopni 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 objednatele, v rámci kterého si osvojí všechny úkony spojené s použitím základních funkcí HSS, byli schopni na svém pracovišti spravovat systém po stránce nastavování jednotlivých scénářů, 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 HSS na svých pracovištích ve FNOL;
* u všech školení dodání zápisu s jmenovitým seznamem proškolených osob a obsahem školení;
* 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 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 svolávací systém řádně bez závad a nedodělků fungovat v ostrém provozu a bude oběma stranami akceptována podpisem protokolu o provedení implementace.

Poskytovatel zahájí plnění předmětu zakázky okamžitě po oboustranném podpisu smlouvy (analýza) a implementuje svolávací systému v **plné** míře výše uvedených požadavků a funkcionalit nejpozději do 2 měsíců od zahájení.

**7. Servisní podpora**

Požadavky na servisní podporu jsou popsány v Příloze č. 4 – Návrh Smlouvy o poskytování služeb technické podpory a servisu a v SLA jako příloha č.1 uvedené smlouvy.