Príloha č. 1 – Opis predmetu zákazky

Verejný obstarávateľ Hlavné mesto Slovenskej republiky Bratislava zadáva zákazku s názvom „Rozvoj a prevádzka informačného systému mestskej polície ŽandárIS“. Kompletné informácie o predmetnej zákazke nájdete na tejto adrese:

https://josephine.proebiz.com/sk/tender/81287/summary

1. Stručný opis predmetu zákazky:

Predmetom zákazky je prevzatie a rozvoj informačného systému Mestskej polície hlavného mesta Slovenskej republiky Bratislava (ďalej len „mestská polícia“) ŽandarIS, ktorý je určený na evidovanie, uchovávanie a spracovávanie výsledkov činnosti mestskej polície, v ktorom sa evidujú všetky udalosti, ktoré boli oznámené tretími osobami alebo boli zistené vlastnou činnosťou príslušníkmi mestskej polície v rámci výkonu služby, ich právna kvalifikácia a spôsob ich vybavenia.

2. Zoznam príslušných CPV kódov:

48810000-9	Informačné systémy
72000000-5	Služby informačných technológií: konzultácie, vývoj softvéru, internet a podpora
72267100-0	Údržba programového vybavenia (softvér) informačných technológií

3. Podrobný opis predmetu zákazky:

I. Predstavenie kontextu

Kedy ako v akom rozsahu sa začal používať IS.

Informačný systém sa používa od roku 2023 vo webovej aplikácii a v roku 2024 bol rozšírený o modul mobilnej aplikácie. Informačný systém vznikal kombináciou interného a externého vývoja, pričom od roku 2025 je plne v internej správe. Po plnom prevzatí bola priorita najmä na odstránení časti technologického dlhu a nutných funkčných opravách. Vzhľadom na nedostatok interných kapacít a iné rozvojové priority bol rozvoj dočasne pozastavený až do momentu vysúťaženia externého dodávateľa. Od cca jesene 2025 je riešenie čisto v prevádzkovom režime.

Cieľom súťaže je nájsť stabilného partnera, ktorý bude schopný prevziať existujúce riešenie, vykonať audit jeho momentálneho technického a bezpečnostného stavu, zabezpečiť jeho prevádzku a bude v ďalšej vlne dovývoja spolupracovať s business ownerom na strane HMBA a pracovať na výstupoch z auditu a sprioritizovaných taskoch podľa backlogu.

Verejný obstarávateľ hľadá takého zmluvného partnera, s ktorým bude pravidelne komunikovať a hľadať najvhodnejšie spôsoby riešenia, vzhľadom na to sa verejný obstarávateľ rozhodol neobmedzovať budúceho dodávateľa v spôsobe dosiahnutia cieľa, ale stanoviť požadovanú výslednú kvalitu.

II. Reálny momentálny technický stav aplikácie

Momentálny stav systému

Od jesene 2025 bol systém v čisto prevádzkovom režime. Používané knižnice a systémy potrebujú update, prípadne k nim existujú otvorené CVEs. V kóde tiež absentuje prísnejšie nastavenie lintovania/typescript validácie. Neexistujú testy (iba základný setup pre unit a pre E2E testy), bezpečnostná ani technická dokumentácia. Neprebehol bezpečnostný audit (ani automatizovaný). Neexistuje monitoring chýb (logov) na frontende aplikácie. Na BE je logovanie minimálne a často nedostatočné na zistenie príčiny zlyhania, a v monitorovacích nástrojoch chýbajú upozornenia na chyby, okrem celkových zlyhaní aplikácie alebo integrácie.

História incidentov

Väčšina incidentov súvisí s výpadkami 3. strán alebo magistrátnej siete, incidenty súvisiace so samotnou aplikáciou ŽandárIS, ktorá je predmetom SLA. Podľa tabuľky nižšie môžeme vidieť dva zaznamenané incidenty spôsobených aplikačnými problémami za posledné dva kalendárne roky.

	Kategórie	1.1.2025-31.12.2025		1.1.2026-31.5.2026	
DEUS / DCOM	integrácie 3. strán	17	63%	8	42%
EVO	integrácie 3. strán	1	4%	3	16%
IMIS / Internet / Mobilné zariadenia / Sieť	sieťové problémy	3	11%	7	37%
Pátranie	integrácie 3. strán	4	15%	1	5%
Žandaris	aplikačné problémy	2	7%	0	0%

Dostupnosť, používatelia, kritickosť

Ide o internú aplikáciu mestskej polície. Mesačne má do 100 aktívnych používateľov. Aplikácia je používaná policajnými hliadkami a musí byť dostupná 24/7.

High-level architektúra systému

a) Riešenie pozostáva z frontendovej a backendovej časti webovej aplikácie. Využívajú sa moderné technológie - Next.js, NestJS, PostgreSQL.

b) Frontend je aplikácia Next.js 14 App Router, ktorá slúži ako webové rozhranie pre interný systém. Je jediným konzumentom backendu NestJS. Používatelia pristupujú k systému prostredníctvom webového prehliadača pre počítače (plnohodnotné rozhranie s bočnou navigáciou).

c) Mobilná aplikácia je Kotlin 1.9 integrujúca sa na MSAL EntraID autentifikáciu, po autentifikácii načíta rovnakú frontendovú aplikáciu ako webové rozhranie a pokračuje v ňom.

d) Backend je aplikácia NestJS podporovaná PostgreSQL (prostredníctvom Prisma ORM). Integruje sa s niekoľkými službami SOAP/REST tretích strán.

Viac detailov v prílohe (bod. II.d) FE ARCHITECTURE, (bod. II.e) BE ARCHITECTURE, (bod. V.a) MOBILE ARCHITECTURE).

Zoznam integrácii 3. strán

Aktuálne (produkčne) využívaná integrácie sú:
- Magproxy – REST, interný systém sprostredkujúci integráciu na štátne registre (RFO,RPO,NEV,RA).
- MinIO S3 (self-hosted) – REST, ukladanie súborov a fotografií.
- Microsoft Entra ID - autentifikácia a manažment používateľov.

Okrem nich existuje v systéme príprava na integráciu na:
- CESDAP_LUST, CESDAP_ZAP – SOAP, štátne systémy ministerstva vnútra - lustrácie vozidel a osôb, zápis priestupkov.
- Enforcement Backoffice – REST, interný systém na vymáhanie pokút z parkovania.

CI/CD/deployment

Mobilná aplikácia neobsahuje CI/CD, deployment procesom je tu manuálny lokálny build a následné odoslanie administrátorovi na bratislavskom magistráte. Webová aplikácia a server sú deployované na magistrátny kubernetes cluster (Tanzu VMware fungujúci on-premise). K aplikačnému namespaceu dostane dodávateľ prístup. Aplikačné clustre sú 3, pre každé prostredie jeden - development, staging, production. Našou CI/CD pipeline sú Github actions, repozitár bude sprístupnený namagistrátnom Github-e. Súčasťou CI je dnes iba úspešná kompilácia frontendu a backendu aplikácie (z typescript-u) a úspešný build. V rámci CD je aplikácia (FE a BE zvlášť) kontajnerizovaná, docker kontajner nahraný na bratislavský Docker Harbor (tiež bežiaci na rovnakom on-premise kubernetes). Kubernetes resources náležiace aplikácii sú manažované cez Kustomise v rámci repozitára. Výnimkou je CNPG postgres databázový cluster, ktorý je spolu s ostatnými magistrátnymi Postgres databázami manažovaný z centrálneho repozitára prostredníctvom Terraform-u. Opäť vie byť umožnený prístup. V rámci deploymentu sa využíva aj interný nástroj (dostupný dodávateľovi, open-source) ktorý sa stará najmä o replacement env variables v Kustomize .yaml súboroch aj .env súboroch podľa deployment prostredia. Tento je však deprecated a po prevzatí ho odporúčame v CI pipeline nahradiť.

Monitoring

Logy a metriky z aplikácie sú odosielané a sledovateľné cez monitorovacie nástroje Grafana/Loki/Prometheus, ku ktorým bude udelený prístup. Alerting je na základe týchto logov a metrík nastaviteľný v aplikácii Grafana.

Dáta a výkon

Aplikácia v produkcii využíva jeden bežiaci "server" (pod) pre BE a jeden pre FE, s nasledovnými zrojmi:

Backend NestJS App

```
resources:
  limits:
    cpu: '1'
```

```
        memory: 2Gi
      requests:
        cpu: 100m
        memory: 256Mi
```

Backend NextJS App

```
      resources:
        limits:
          cpu: '1'
          memory: 2Gi
        requests:
          cpu: 50m
          memory: 128Mi
```

Okrem nich využíva CNPG Posgres databázový cluster, s dvoma replikami (v dvoch data centrách v tom istom kubernetes clustri) a nasledovnými zdrojmi.

```
  limits:
    cpu: '2'
    memory: 6Gi
  requests:
    cpu: '2'
    memory: 6Gi
```

Databáza obsahuje 4gb dát v rátane osobných údajov občanov, približne 400gb statických dát (fotiek/dôkazov) sa nachádza v self-hoste minio (S3) bucket-e.

III. Audit a stabilizácia systému

Cieľom tejto fázy je získať objektívny prehľad o stave systému a definovať prioritizované kroky na jeho stabilizáciu a ďalší rozvoj.

Ide o samostatnú jednorázovú fázu, ktorá zahŕňa:

a) technický audit,
b) bezpečnostný audit,
c) prevádzkový audit,
d) audit dokumentácie,
e) identifikáciu technického dlhu,
f) onboarding a knowledge transfer,
g) návrh stabilizačnej roadmapy.

Počiatočný audit bude pozostávať minimálne z nižšie popísaných súčastí. Prvé výstupy a odporúčania budú dodané do 10 pracovných dní od sprístupnenia zdrojových kódov, existujúcej dokumentácie a potrebných prístupov. Kompletné výsledky budú prezentované **do 4 týždňov**, formou **odovzdanej dokumentácie**, a tiež stretnutia alebo workshopu s vývojárskym tímom aj zástupcami obstarávateľa. Verejný obstarávateľ poskytne dodávateľovi dostupné podklady potrebné na prevzatie riešenia, najmä zdrojové kódy, dostupnú technickú dokumentáciu, popis architektúry riešenia, zoznam integrácií na tretie strany, popis deployment procesu, prístup do monitorovacích nástrojov a dostupné prevádzkové

informácie v rozsahu primeranom možnostiam verejného obstarávateľa. V prípade potreby si dodávateľ vyžiada ďalšie podklady alebo súčinnosť nevyhnutnú na riadne vykonanie úvodnej analytickej fázy. Verejný obstarávateľ požaduje, aby budúci dodávateľ disponoval kapacitami pre samostatné bezpečnostné posúdenie pokrývajúce aplikačnú aj infraštruktúrnu vrstvu a bol schopný výsledky dodať spolu s technickým auditom bez závislosti na existujúcej bezpečnostnej dokumentácii.

Formát výsledného dokumentu bude ponechaný na dodávateľa, súčasťou úvodného auditu musí byť:

a) **Technický audit** - pokrývajúci kvalitu kódu, pokrytie automatizovanými testami, vývojové a nasadzovacie procesy, infraštruktúru, integrácie tretích strán a bezpečnosť závislostí. Výsledkom bude dokument obsahujúci manažérske zhrnutie, technické zistenia s maticou rizík podľa závažnosti, identifikáciu technického dlhu a prioritizovaný plán nápravných krokov. Súčasťou bude aj identifikácia oblastí so zvýšenou závislosťou na nedostatočne zdokumentovaných znalostiach alebo kritických osobných znalostiach.

b) **Bezpečnostné posúdenie** - pokrýva autentifikáciu a autorizáciu, model rolí a oprávnení, audit logy, šifrovanie dát a bežné aplikačné zraniteľnosti. Výstupom je bezpečnostný report s nálezmi klasifikovanými podľa závažnosti a priorizovanými odporúčaniami. Posúdenie primerane zohľadní aj aktuálnosť používaných technológií a aktualizačný režim kritických komponentov riešenia.

c) **Prevádzkový audit a stabilizačná roadmapa** - audit infraštruktúry, monitoringu, logovania, spracovania chýb a alertingu začne bezprostredne po prevzatí prístupov. Pri riešeniach s integráciami na tretie strany bude súčasťou posúdenia aj návrh spôsobu rozlíšenia pôvodu incidentov a odporúčanie evidencie incidentov podľa aplikačnej, infraštruktúrnej alebo externej príčiny. Kompletná roadmapa stabilizácie bude dodaná spolu s výsledkami technického auditu. Stabilizačné opatrenia budú navrhnuté ako prioritizované zásahy nevyhnutné na odstránenie identifikovaných rizík bez neprimeraného dopadu na funkčný rozsah alebo dostupnosť riešenia.

d) **Odporúčanie rozvojovej stratégie** - odporúčanie, či je pre daný systém vhodnejší priebežný rozvoj, čiastočný refaktoring alebo väčší architektonický zásah. Odporúčanie musí byť odôvodnené analýzou technického dlhu, miery závislostí, testovateľnosti, frekvencie incidentov a nákladov na údržbu v porovnaní s nákladmi na zásah, pričom zohľadní strednodobú rozvojovú roadmapu systému. Odporúčanie bude zároveň reflektovať potrebu zachovania kontinuity prevádzky a minimalizácie dopadu navrhovaných opatrení na používateľov systému.

Navrhnutú štruktúru môže dodávateľ ďalej rozšíriť alebo upraviť podľa svojho metodického prístupu. Vybrané opatrenia na zníženie technického dlhu alebo odstránenie identifikovaných rizík budú po vzájomnej dohode Zmluvných strán realizované postupne v rámci SLA služieb alebo rozvojových aktivít.

IV. SLA / prevádzková podpora

Dodávateľ sa zaväzuje poskytovať verejnému obstarávateľovi služby prevádzky, podpory a riadenia incidentov informačného systému ŽandárIS (ďalej len „SLA služby“).

SLA služby nezahŕňajú rozvojové aktivity (najmä vývoj nových funkcionalít, zásadné zmeny architektúry alebo rozširovanie rozsahu systému), ktoré sú predmetom samostatného plnenia.

Dodávateľ je povinný zabezpečiť, aby poskytovanie SLA služieb neviedlo k duplicitnému účtovaniu kapacít vo vzťahu k rozvojovým aktivitám. Kapacity využívané na rozvoj systému nesmú byť súčasne účtované ako SLA kapacity, pokiaľ sa nejedná o výslovne objednané SLA služby.

Dodávateľ začína poskytovať SLA služby najskôr po ukončení auditu a po formálnom prevzatí systému do prevádzkovej podpory. Počas realizácie rozsiahlych rozvojových aktivít môžu Zmluvné strany písomne dohodnúť dočasné obmedzenie vybraných SLA služieb vo vzťahu ku konkrétnym rozvíjaným komponentom systému.

Takéto obmedzenie musí byť vždy časovo ohraničené, písomne odsúhlasené Objednávateľom a nesmie mať negatívny dopad na prevádzku ostatných častí Informačného systému.

Rozsah SLA služieb

SLA služby zahŕňajú najmä

Monitoring dostupnosti a detekcia incidentov

- Zabezpečenie automatizovaného monitoringu dostupnosti všetkých produkčných komponentov informačného systému vrátane aplikačnej vrstvy, databázy, integračných rozhraní a ďalších kritických služieb nevyhnutných na riadnu prevádzku systému.
- Sledovanie dostupnosti integračných rozhraní a externých služieb.
- Nastavenie alertingu pri chybách a výpadkoch.
- Proaktívna informovanosť verejného obstarávateľa o kritických a bezpečnostných incidentoch s dopadom na používateľov.

Na monitorovanie a alerting bude možné využiť existujúci systém verejného obstarávateľa (Grafana, Loki, Prometheus).

Primárnym zdrojom údajov pre vyhodnocovanie dostupnosti systému, plnenia SLA a riešenie sporov sú údaje z monitorovacieho systému verejného obstarávateľa, pokiaľ sa zmluvné strany nedohodnú inak.

Dostupnosť systému a meranie dostupnosti

Dodávateľ musí zabezpečiť prevádzku Informačného systému v režime 24 hodín denne, 7 dní v týždni a garantovať jeho dostupnosť najmenej na úrovni 99,5 % za každý kalendárny mesiac. Úroveň 99,5 % zodpovedá maximálne cca 3 hod 40 min. nedostupnosti mesačne.

Dodávateľ musí zabezpečiť automatizované meranie dostupnosti monitorovacím nástrojom v rámci SLA služieb, sprístupniť verejnému obstarávateľovi priebežný prístup k údajom o dostupnosti a uvádzať dosiahnutú dostupnosť v pravidelnom mesačnom reporte. Na požiadanie poskytne zdrojové logy meraní.

Výpočet dostupnosti:

Dostupnosť (%) = (T − V − N) / (T − V) × 100,

kde T = jeden kalendárny mesiac, V = vylúčený čas, N = čas nedostupnosti.

Dostupnosť = stav, v ktorom je systém a jeho kľúčové funkcie prevádzkyschopný a použiteľný pre používateľov v súlade s jeho určením.

Nedostupnosť = stav, keď systém alebo jeho kľúčová funkcia nie je použiteľná (úplná nedostupnosť), alebo je použiteľná len s podstatne zhoršeným výkonom oproti požadovaným parametrom (čiastočná nedostupnosť); čiastočná nedostupnosť sa započítava koeficientom [0,5].

Vylúčený čas = Do času nedostupnosti sa nezapočítava obdobie:

- Plánovanej údržby vopred oznámenej a odsúhlasenej podľa požiadaviek na plánovanú údržbu.
- Výpadku služieb tretích strán (najmä DEUS, IMIS, sieťová infraštruktúra) mimo sféry vplyvu dodávateľa.
- Vyššej moci alebo konania či zavinenia verejného obstarávateľa alebo používateľov.

Nedodržanie garantovanej úrovne dostupnosti je porušením povinnosti dodávateľa, s ktorým sú spojené sankcie podľa príslušného článku návrhu zmluvy (zmluvné pokuty viazané na cenu Paušálnej služby za dotknuté Merné obdobie).

Spracovanie chýb a logovanie

- Zabezpečenie jednotného mechanizmu zachytávania chýb.
- Logovanie chýb a udalostí na úrovni frontend aj backend.
- Zabezpečenie uchovávania auditných záznamov o bezpečnostne významných operáciách a administrátorských zásahoch.
- Zabezpečenie dohľadateľnosti príčiny incidentu vrátane väzby na konkrétnu transakciu alebo integračný tok.

Chyby prezentované používateľovi musia obsahovať zrozumiteľnú informáciu a jednoznačný identifikátor umožňujúci ich dohľadanie. Chybové hlásenia nesmú používateľovi sprístupniť citlivé technické ani bezpečnostné informácie. Verejný obstarávateľ sprístupní dodávateľovi existujúci portál pre monitorovanie aplikácii (Grafana), integrovaný na logy (Loki) a metriky (Prometheus) aplikácii. Dlhodobé uchovávanie a dohľadateľnosť logov a metrík zabezpečuje verejný obstarávateľ. Bez ohľadu na dodávatelom používaný systém (najmä v prípade frontendových logov), musia byť zbierané logy odosielané do systému verejného obstarávateľa na dlhodobé uchovávanie.

V prípade dočasnej nedostupnosti monitorovacieho systému verejného obstarávateľa je Dodávateľ povinný zabezpečiť dočasné uchovanie logov a ich automatizované alebo bezodkladné odoslanie po obnovení dostupnosti monitorovacieho systému.

Incident management a on-call podpora

- Prijatie a evidencia incident.
- Klasifikácia incidentu podľa závažnosti.
- Potvrdenie kategórie incidentu verejnému obstarávateľovi.
- Aktivácia primeranej reakcie podľa závažnosti incidentu vzhľadom na servisné okno.
- Diagnostika príčiny incidentu v rozsahu primeranom dostupným informaciám.
- Koordinácia riešenia incident až do jeho neutralizácie, resp. trvalého vyriešenia.
- Eskalácia incidentov voči tretím stranám (najmä DEUS, IMIS, sieťová infraštruktúra).
- Priebežné informovanie verejného obstarávateľa o stave incidentu.

Dodávateľ je povinný poskytnúť verejnému obstarávateľovi sprístupniť systém na evidenciu incidentov v potrebnom rozsahu. Počas trvania aj po ukončení spolupráce je povinný na vyžiadanie poskytnúť

export dát v strojovo čitateľnej podobe. V prípade, že počas trvania spolupráce verejný obstarávateľ predstaví adekvátnu náhradu tohto riešenia, bude Dodávateľovi umožnený dostatočný čas na prechod na nové riešenie. Dodávateľ je povinný vytvoriť a priebežne udržiavať číselník chybových kódov dostupný 24/7, ktorý bude slúžiť ako referenčný zdroj pri nahlasovaní incidentov v rámci SLA. Logovanie chýb musí umožniť spätné dohľadanie technickej príčiny vrátane väzby na konkrétnu transakciu alebo integračný tok.

Incident management musí zabezpečovať rozlíšenie incidentov podľa ich pôvodu (aplikačný, infraštruktúrny, integračný) a primeranú koordináciu s dotknutými subjektmi. Dodávateľ je zodpovedný za riadenie incidentu bez ohľadu na jeho príčinu. V prípade incidentov spôsobených externými službami zabezpečuje Dodávateľ koordináciu a eskaláciu, nie je však zodpovedný za samotné odstránenie príčiny. Lehoty na neutralizáciu a trvalé vyriešenie Incidentu sa v takom prípade neuplatňujú, ak Poskytovateľ preukázateľne vykonal všetky primerané kroky na identifikáciu, eskaláciu a koordináciu riešenia Incidentu voči príslušnej tretej strane. Verejný obstarávateľ poskytne kontaktné osoby na integrácie 3. strán.

Servisné okno

Servisné okno sa stanovuje rozdielne podľa závažnosti Incidentu nasledovne:

Kategória Incidentu	Servisné okno	Režim
Bežné incidenty	Pracovné dni v čase od 8:00 do 16:00	8 × 5
Kritické incidenty	Pracovné dni, v čase od 7:00 do 22:00	15 x 5

Reakčné časy

Ak je Incident nahlásený mimo prebiehajúceho servisného okna platného pre danú kategóriu Incidentu, lehota na reakciu plynie od začiatku najbližšieho servisného okna.

Pri Bezpečnostných incidentoch, pre ktoré je stanovené servisné okno v režime 24 × 7, lehoty plynú vždy od okamihu nahlásenia bez ohľadu na deň alebo hodinu.

Pri incidentoch zapríčinených treťou stranou sa berú do úvahy lehoty na reakciu, resp. eskaláciu incidentu. Na Dodávateľa sa v týchto prípadoch nevzťahujú lehoty na neutralizáciu, resp. trvalé vyriešenie incidentu.

Nasledujúca tabuľka má ***informatívny charakter*** *a slúži na lepšiu orientáciu. Záväzné lehoty sú stanovené v príslušnom článku Zmluvy o riešení Incidentov; v prípade rozporu má prednosť znenie Zmluvy.*

Kategória	Reakcia	Neutralizácia	Trvalé vyriešenie	Okno
Bežný incident	do 4 hodín	do 2 prac. dní	do 5 prac. dní	8 × 5
Kritický incident	do 30 minút	do 4 hodín	do 24 hodín	**15 x 5**

Root Cause Analysis (RCA)

Pri incidentoch je Dodávateľ povinný vypracovať analýzu koreňovej príčiny (RCA), ktorá obsahuje:

- Popis incidentu a jeho priebeh.
- Identifikáciu príčiny.
- Zhodnotenie dopadu.
- Prijaté opatrenia.
- Odporúčania na prevenciu opakovania.

Závažnosť incidentu	Lehota na doručenie RCA
Kritický incident	do 72 hodín od trvalého vyriešenia
Bezpečnostný kritický incident	**do 24 hodín od trvalého vyriešenia**

V odôvodnených prípadoch môže byť RCA report v stanovenej lehote predložený v predbežnej verzii. Finálna verzia bude doručená bez zbytočného odkladu po potvrdení koreňovej príčiny Incidentu.

Údržba systému (Maintenance)

Dodávateľ zabezpečuje priebežnú technickú údržbu systému v rozsahu:

- Aktualizácia knižníc a technických závislostí.
- Aplikácia bezpečnostných a systémových patchov.
- Odstraňovanie známych zraniteľností.
- Zabezpečenie kompatibility a stability systému.

Pri vykonávaní zmien, ktoré môžu ovplyvniť prevádzku informačného systému, je Poskytovateľ povinný mať pripravený rollback postup umožňujúci návrat k poslednému stabilnému stavu systému v prípade neúspešného nasadenia alebo závažných prevádzkových problémov

Údržba systému podľa tohto bodu nezahŕňa zmeny vyžadujúce zásadný zásah do architektúry, implementáciu nových funkcionalít alebo iné činnosti presahujúce bežnú technickú údržbu systému. Takéto činnosti sa považujú za rozvojové aktivity a realizujú sa na základe samostatnej objednávky.

Plánovaná údržba

Plánované servisné zásahy a údržbu, ktoré môžu mať dopad na dostupnosť Informačného systému, je Dodávateľ povinný:

- Oznámiť verejnému obstarávateľovi vopred, najneskôr **5 pracovných dní** pred ich vykonaním, s uvedením predpokladaného času a dĺžky trvania.
- Vykonávať iba po predchádzajúcom súhlase od verejného obstarávateľa a overení, že čas zásahu nekoliduje so zvýšenou potrebou bezpečnosti (napr. počas veľkých kultúrnych a/alebo športových podujatí).

Výnimka platí iba pre neodkladné bezpečnostné zásahy, ktoré musia byť Dodávateľom jasne zdôvodnené.

Po ukončení plánovaného zásahu je Dodávateľ povinný bezodkladne informovať verejného obstarávateľa o úspešnom ukončení údržby a obnovení štandardnej prevádzky.

Drobné opravy

SLA služby zahŕňajú realizáciu drobných opráv systému (max. 5MD mesačne), ktoré nepredstavujú rozvoj:

- Bugfixy a opravy chýb.
- Konfigurácie a malé úpravy správania systému.

Do rozsahu drobných opráv sa nezapočítava odstraňovanie incidentov a vád, ktoré sú súčasťou SLA služieb. Po vyčerpaní mesačného limitu drobných opráv budú ďalšie práce realizované iba na základe samostatnej objednávky alebo po vzájomnej dohode zmluvných strán.

Dokumentácia

Dodávateľ je povinný:

- Priebežne aktualizovať technickú dokumentáciu systému.
- Aktualizovať prevádzkovú dokumentáciu.
- Udržiavať dokumentáciu v stave umožňujúcom prevzatie systému bez neprimeraných nákladov.
- Držať túto dokumentáciu v git repozitáry spolu so zvyškom zdrojových kódov.

Dokumentácia musí zodpovedať aktuálnej produkčnej verzii systému. Dokumentácia je považovaná za aktuálnu až po revízii obstarávateľom, prípadnom zapracovaní pripomienok a následnom schválení.

SLA reporty

Reporty sa vyhotovia minimálne raz mesačne ako podklad pre vyhodnotenie plnenia SLA. Musia byť odoslané najneskôr do 5 dňa nasledujúceho kalendárneho mesiaca a musia obsahovať:

- Merné obdobie, dátum vyhotovenia.
- Dosiahnutá dostupnosť (podľa definovaného vzorca) v % vs. garantovaná úroveň.
- Celkový čas nedostupnosti, z toho úplná a čiastočná (so započítaním koeficientu), vylúčený čas a jeho dôvod.
- Počty incidentov podľa kategórie (bežný / kritický / bezpečnostný) a podľa pôvodu (aplikačný / infraštruktúrny / integračný).
- Zoznam incidentov s jednotlivými aj priemernými časmi reakcie / neutralizácie / vyriešenia a označením splnené/nesplnené. (pri incidentoch zapríčinených treťou stranou sa nevzťahujú lehoty).
- Čerpanie drobných opráv (v MD).
- Stručný zoznam vykonaných aktívi na údržbu, odstránenie zraniteľností.

V kvartálnej frekvencii poskytne Dodávateľ aj opakujúce sa trendy / problémy / rizikové miesta a odporúčania, resp. návrhy preventívnych opatrení.

V. Plánovaný rozvoj

Rozvojové oblasti sú bližšie popísané v separátnom dokumente MSP Backlog.docx. Backlog slúži ako referenčný podklad pre nacenenie a nastavenie spolupráce, pričom jeho obsah nie je záväzný a môže byť priebežne upravovaný. Backlog obsahuje 4 prioritné požiadavky a viac ako 30 zvyšných úloh. Úlohy budú detailnejšie popísané po prevzatí systému.

Vzhľadom na rozpočtové obmedzenie a zatiaľ neznáme výstupy z auditu bude plán rozvoja a prioritizácia sfinalizovaná až po odprezentovaní výstupov z auditu. Estimácia úloh bola stanovená ako

odhad na základe súčasného poznania systému. Úlohou dodávateľa bude po oboznámení sa so systémom a pred ukončením auditu tieto odhady potvrdiť alebo upraviť.

Rozvoj systému bude riadený oddelene od stabilizačnej fázy a bežnej prevádzky. Uprednostňuje sa agilný alebo hybridný spôsob riadenia, pričom rozsah rozvoja nebude fixovaný vopred, ale bude riadený prostredníctvom backlogu a dostupných kapacít.

Záväzky verejného obstarávateľa

a) **Jasne definovaný Business / Product Owner,** ktorý bude mať mandát rozhodovať o prioritách backlogu, kompetenciu akceptovať alebo neschvaľovať výstupy, možnosť rýchlo riešiť otázky týkajúce sa biznis logiky a právomoc robiť ad-hoc rozhodnutia počas nábehu a stabilizačnej fázy. Business Owner bude dodávateľovi k dispozícii počas celého trvania spolupráce.

b) **Dostupnosť interných technických expertov počas úvodnej fázy –** verejný obstarávateľ zabezpečí počas úvodnej fázy prevzatia systému dostupnosť interného experta (8/5), ktorý má znalosť aktuálneho riešenia a súčinnosť pri vysvetlení architektúry, procesu nasadzovania, biznisových tokov a histórie incidentov, knowledge transfer počas prvej fázy a možnosť konzultovať otázky súvisiace s predchádzajúcou implementáciou. Dostupnosť bude v rozsahu primeranom potrebám projektu, najviac však 10 hodín týždenne. Ak interný tím nie je dostupný, bude možné akceptovať dlhšie trvanie technického auditu.

c) **Realistické očakávania počas úvodnej fázy –** verejný obstarávateľ akceptuje, že prevzatie riešenia **neznamená okamžitý rozvoj nových funkcionalít**, prvé 6–8 týždňov bude venovaných auditu, rekonštrukcii znalostí, stabilizácii a doplneniu dokumentácie, prvotné investície do stabilizácie sú nevyhnutné a nesmú byť považované za "práce navyše".

d) **Pripravený a prístupný backlog s jasnou prioritizáciou –** verejný obstarávateľ musí zabezpečiť existujúci zoznam známych incidentov, chýb a požiadaviek, priorizáciu backlogu zo strany Business Ownera, jednotné akceptačné kritériá a súčinnosť pri testovaní pre všetky úlohy, stabilitu požiadaviek v rámci sprintu, definované procesy pre schvaľovanie a zmeny priorít. Bez jasného backlogu nie je možné efektívne plánovať sprinty, rozvoj a stabilizáciu.

Záväzky dodávateľa

a) **Skúsenosti s citlivými systémami** verejný obstarávateľ identifikoval ako kľúčovú požiadavku skúsenosť s implementáciou alebo prevádzkou informačných systémov pracujúcich s citlivými údajmi alebo systémov závislých od externých registrov, pričom **vyžaduje, aby takéto plnenia boli realizované v súlade s príslušnými bezpečnostnými štandardmi**. Z tohto dôvodu sa verejný obstarávateľ rozhodol zamerať na stanovenie požadovanej výslednej kvality plnenia, bez obmedzovania konkrétneho spôsobu jej dosiahnutia.

b) **Pripravenosť na odovzdanie** Dodávateľ je povinný počas celej doby spolupráce udržiavať projekt v stave umožňujúcom jeho prevzatie obstarávateľom alebo iným dodávateľom bez

neprimeraných nákladov alebo rizík. Dokumentácia architektúry, procesov a biznis logiky musí byť aktualizovaná, odovzdávaná, a schvaľovaná obstarávateľom priebežne nie až na konci spolupráce. Súčasťou priebežnej dokumentácie musí byť aj evidencia kritických prevádzkových rozhodnutí a zmien architektúry prijatých počas spolupráce.

c) **Personálne obsadenie tímu** Dodávateľ zabezpečí odborné kapacity, ktorých rozsah a seniorita musia zodpovedať rozsahu prác ak, aby bolo možné zabezpečiť všetky činnosti súvisiace s prevzatím riešenia, auditom, stabilizáciou, rozvojom, prevádzkou, bezpečnosťou a riešením incidentov.

Popisy rolí

Tech Lead (0,5 – 1 FTE)

Zodpovednosť role

Zodpovedá za technické vedenie realizačného tímu, architektúru riešenia a technickú kvalitu dodávaného systému.

Hlavné činnosti

- Navrhuje architektúru a technickú koncepciu riešenia.
- Stanovuje technické štandardy a dohliada na ich dodržiavanie.
- Koordinuje prácu vývojového tímu, prideľuje technické úlohy, vykonáva technickú validáciu navrhovaných riešení a code review.
- Navrhuje refaktoring, rieši komplexné technické incidenty (L3) a riadi odstraňovanie technického dlhu.
- Podieľa sa na technickom prevzatí riešenia od existujúceho dodávateľa, vyhodnocuje jeho technický stav a navrhuje stabilizačný plán (roadmapu).
- Posudzuje technické dopady zmenových požiadaviek a poskytuje objednávateľovi odborné odporúčania pri rozhodovaní o ďalšom rozvoji systému.

Požadovaný profil

Seniorný technický špecialista so skúsenosťami s návrhom architektúry informačných systémov, vedením vývojového tímu a implementáciou zmien v produkčných aplikáciách. Musí mať skúsenosti s technológiami **Next.js, NestJS, TypeScript, PostgreSQL**, návrhom REST API, code review a návrhom škálovateľných architektúr. Výhodou sú skúsenosti s cloudovými platformami, kontajnerovými technológiami a CI/CD.

Fullstack vývojár (1 – 2 FTE)

Zodpovednosť role

Zodpovedá za návrh, vývoj a údržbu frontendovej aj backendovej časti riešenia.

Hlavné činnosti

- Implementuje nové funkcionality a zmeny vyplývajúce z požiadaviek objednávateľa, roadmapy, backlogu alebo výsledkov funkčných či bezpečnostných auditov.
- Vyvíja frontendové aj backendové časti aplikácie vrátane integračných rozhraní voči systémom tretích strán (REST/SOAP).

- Podieľa sa na optimalizácii výkonu, odstraňovaní technického dlhu, riešení incidentov a stabilizácii systému.
- Spolupracuje pri návrhu, testovaní, dokumentovaní a nasadzovaní zmien.

Požadovaný profil

Vývojár minimálne na úrovni **medior** so skúsenosťami s technológiami **Next.js (App Router), NestJS, TypeScript, Prisma, PostgreSQL**, návrhom REST API, Git a prácou v agilne riadenom vývojovom tíme.

DevOps inžinier (0 – 0,5 FTE)

Zodpovednosť role

Zodpovedá za automatizáciu nasadzovania, správu infraštruktúry a zabezpečenie spoľahlivej, bezpečnej a stabilnej prevádzky riešenia.

Hlavné činnosti

- Navrhuje, spravuje a rozvíja CI/CD pipeline a zabezpečuje nasadzovanie nových verzií aplikácie.
- Spravuje vývojové, testovacie a produkčné prostredia vrátane cloudovej infraštruktúry, kontajnerových platforiem a súvisiacich komponentov.
- Zabezpečuje monitoring, logovanie, alerting a sledovanie dostupnosti interných aj externých služieb.
- Podieľa sa na analýze prevádzkových incidentov a navrhuje opatrenia vedúce k zvýšeniu dostupnosti, bezpečnosti, výkonu a prevádzkovej stability systému.
- Realizuje migračné, stabilizačné a automatizačné aktivity súvisiace s prevádzkou riešenia.

Požadovaný profil

Špecialista minimálne na úrovni **medior** so skúsenosťami v oblasti **DevOps**, cloudovej infraštruktúry, kontajnerových technológií (napr. Docker), orchestrácie kontajnerov (napr. Kubernetes), CI/CD, monitoringu, logovania a prevádzky produkčných systémov.

Ak túto rolu vykonáva tá istá osoba ako **Tech Lead**, musia byť ich zodpovednosti jednoznačne oddelené.

Projektový manažér (0,3 – 0,5 FTE)

Zodpovednosť role

Zodpovedá za riadenie realizácie služieb, koordináciu realizačného tímu a komunikáciu s objednávateľom.

Hlavné činnosti

- Plánuje, koordinuje a riadi rozvojové, prevádzkové a stabilizačné aktivity;
- Organizuje prácu tímu, zabezpečuje agilné riadenie vývoja, plánuje sprinty alebo iný spôsob riadenia vývoja a koordinuje backlog;
- Zabezpečuje komunikáciu s objednávateľom, koordinuje riešenie zmenových požiadaviek, incidentov a ďalších prevádzkových aktivít;

- Riadi projektové riziká, odstraňuje prekážky realizácie a sleduje plnenie zmluvných záväzkov pri poskytovaní služieb;
- Zodpovedá za pravidelný reporting priebehu realizácie vrátane výstupov z auditov, stabilizačných aktivít, incident managementu a plnenia harmonogramu.

Požadovaný profil

Špecialista minimálne na úrovni **medior** so skúsenosťami s riadením IT projektov alebo poskytovaním aplikačnej podpory a rozvoja informačných systémov. Musí mať skúsenosti s koordináciou multidisciplinárnych tímov, riadením dodávky služieb, komunikáciou s objednávateľom, riadením rizík, agilným riadením vývoja (napr. Scrum) a pravidelným reportingom.

Tester (0,3 – 0,7 FTE)

Zodpovednosť role

Zodpovedá za zabezpečenie kvality dodávaného riešenia z hľadiska funkčnosti, stability a pripravenosti na nasadenie.

Hlavné činnosti

- Pripravuje testovaciu stratégiu, testovacie scenáre, testovacie dáta a akceptačné kritériá.
- Vykonáva funkčné, integračné a regresné testovanie.
- Eviduje chyby, overuje reprodukovateľnosť chýb, validuje opravy a schvaľuje zmeny pred ich nasadením.
- Spolupracuje s vývojovým tímom pri analýze incidentov a navrhuje opatrenia na zvyšovanie kvality riešenia.

Požadovaný profil

Špecialista minimálne na úrovni medior so skúsenosťami s testovaním informačných systémov, prípravou testovacích scenárov, správou chýb, validáciou zmien a prácou v agilne riadenom vývojovom tíme. Výhodou sú skúsenosti s nástrojmi na správu testov a evidenciu chýb.

Dostupnosť expertných rolí

Uvedené kapacity jednotlivých rolí (FTE) majú orientačný charakter a slúžia na rámcové vymedzenie očakávaného personálneho pokrytia. Skutočný rozsah zapojenia jednotlivých rolí sa môže počas trvania spolupráce meniť v závislosti od aktuálnych potrieb, najmä intenzity rozvoja, stabilizačných aktivít alebo prevádzkových požiadaviek systému.

Konkrétne rozdelenie kapacít a ich úpravy budú predmetom priebežných dohôd medzi verejným obstarávateľom a dodávateľom s cieľom zabezpečiť efektívne využitie kapacít.

d) Kontinuita a skúsenosti tímu Rotácia členov tímu bez vážnych dôvodov je nežiaduca, a považuje sa za riziko pre zachovanie kontinuity prevádzky a rozvoja.

Dodávateľ musí zabezpečiť:

- Stabilitu kľúčových členov tímu.

- Plánované zmeny personálneho obsadenia len so súhlasom HMBA.
- Náhradníkov s rovnakou alebo vyššou úrovňou kvalifikácie.
- Dokumentáciu umožňujúcu prevzatie riešenia novým členom alebo HMBA bez neprimeraných nákladov.
- Účasť vybraných odborníkov (minimálne projektový manažér, tech lead) na prípadných osobných stretnutiach s business ownerom.

Osobná forma stretnutí sa môže využiť najmä v úvodnej fáze prevzatia riešenia, pri významných architektonických rozhodnutiach, kvartálnych plánovaniach alebo riešení kritických problémov a to po predchádzajúcej dohode. Bežná spolupráca môže po dohode zmluvných strán prebiehať primárne v online režime.

Dodávateľ garantuje, že členovia tímu majú:

- Skúsenosti s projektami podobného rozsahu a charakteru.
- Odbornú znalosť použitého technologického stacku (Next.js, NestJS, PostgreSQL/Prisma, Azure AD).
- Schopnosť fungovať v tíme riadiacom sa agilnými princípmi.
- Schopnosť komunikovať v slovenskom aj v anglickom jazyku.

Pri rolách projektového manažéra a tech leada/architekta sa očakáva schopnosť samostatne viesť odbornú diskusiu a formulovať technické odporúčania vo vzťahu k HMBA. Dodávateľ nie je viazaný pevnou skladbou tímu, je však povinný zabezpečiť požadované kompetencie v potrebnom rozsahu.

Pri plnení predmetu zákazky sa očakáva pravidelná osobná súčinnosť dodávateľa so zástupcami HMBA, najmä pri prevzatí riešenia, architektonických rozhodnutiach, prioritizácii backlogu a riešení kľúčových prevádzkových tém. Online forma spolupráce môže byť využívaná priebežne.

Súvisiace dokumenty sú:

Príloha č. 1 (bod V.a) – opis predmetu zákazky MSP Backlog.docx (informatívny dokument).

Príloha č. 1 (bod V.b) – opis predmetu zákazky Interná smernica č. 37 (informatívny dokument)

Príloha č. 1 (bod V.c) – opis predmetu zákazky Interná smernica č. 41 (informatívny dokument)

Príloha č. 1 (bod II.d) - FE ARCHITECTURE (informatívny dokument)

Príloha č. 1 (bod. II.e) - BE ARCHITECTURE (informatívny dokument)