Prováděcí smlouva č.j. PPR-42481-6/ČJ-2021-990656

k Rámcové dohodě č.j. PPR-22494-18/Čj-2020-990656

Smluvní strany:

Česká republika – Ministerstvo vnitra

Sídlo:	Nad Štolou 936/3, PSČ 170 34, Praha
IČO:	00007064
DIČ:	CZ00007064
Zastoupená:	plk. Mgr. Pavlem Osvaldem, ředitelem Ředitelství pro podporu výkonu služby Policejního prezidia ČR
Bankovní spojení:	Česká národní banka, Praha 1 č.ú. 5504881/0710
Korespondenční adresa:	Policejní prezidium ČR, Ředitelství pro podporu výkonu služby, poštovní schránka 62/ ŘPVS, 170 89 Praha 7

(dále jen „Objednatel“)

a

Be a Future s.r.o.

Sídlo:	Rybná 716/24, Staré Město, 110 00 Praha 1
IČO:	04876041
DIČ:	CZ04876041
Zastoupená:	[redacted] jednatelem společnosti
Bankovní spojení:	Komerční banka, a.s. 115-2165660217/0100
Korespondenční adresa:	Karlovo náměstí 8/313, Nové Město, 120 00 Praha 2

Obchodní společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 285925

(dále jen „Dodavatel“)

(společně dále také jen „Smluvní strany“, nebo jednotlivě „Smluvní strana“)

uzavřely tuto Prováděcí smlouvu (dále jen „Prováděcí smlouva“) k Rámcové dohodě PPR-22494-18/Čj-2020-990656, ze dne 13.11.2020 (dále jen „Rámcová dohoda“) v souladu s ustanoveními zákona č. 89/2012 Sb., občanský zákoník, (dále jen „občanský zákoník“) a zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ) k veřejné zakázce s názvem „**Technická podpora a provoz MBP z RD 2022 - fixní část**“. č.j. PPR-42481/ČJ-2021-990656.

1. PŘEDMĚT SMLOUVY

1.1. Předmětem této Prováděcí smlouvy je závazek Dodavatele poskytnout Objednateli plnění v souladu se specifikací uvedenou v Příloze č. 1 této Prováděcí smlouvy (dále též jen „Plnění“).

1.2. Objednatel se zavazuje řádně dodané Plnění převzít a zaplatit za něj dohodnutou cenu, a to způsobem definovaným v této Prováděcí smlouvě a v Rámcové dohodě.

2. CENA

2.1. Celková cena za Plnění dle této Prováděcí smlouvy činí 17 340 000,00 Kč bez DPH, a 20 981 400,00 Kč s DPH. Cena za jednotlivé položky Plnění je uvedena v Příloze č. 2 této Prováděcí smlouvy.

2.2. Dodavatel je oprávněn vystavit fakturu za poskytnuté dílčí plnění, a to vždy za uplynulé kalendářní čtvrtletí, na základě dílčího akceptačního protokolu.

3. TERMÍN PLNĚNÍ A MÍSTO PLNĚNÍ

3.1. Dodavatel je povinen dodat předmět plnění v období od 1. 1. 2022 do 31. 12. 2022, pokud v Příloze č. 1 není stanoveno jinak.

3.2. Místem plnění je Bubenečská 20, Praha 6.

3.3. Adresa Objednatele pro doručení daňového dokladu je:

Policejní prezidium ČR, Ředitelství pro podporu výkonu služby,
Strojnická 27, poštovní schránka 62/ŘPVS, 170 89 Praha 7

4. OSTATNÍ UJEDNÁNÍ

4.1. Veškerá ujednání této Prováděcí smlouvy navazují na Rámcovou dohodu a podmínkami uvedenými v Rámcové dohodě se řídí, tj. práva a povinnosti či skutečnosti neupravené v této Prováděcí smlouvě se řídí ustanoveními Rámcové dohody. V případě, že ujednání obsažené v této Prováděcí smlouvě se bude odchylovat od ustanovení obsaženého v Rámcové dohodě, má ujednání obsažené v této Prováděcí smlouvě přednost před ustanovením obsaženým v Rámcové dohodě, ovšem pouze ohledně plnění sjednaného v této Prováděcí smlouvě.

4.2. Tato Prováděcí smlouva nabývá účinnosti dnem uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

4.3. Tato Smlouva je vyhotovena tak, že je podepsána oběma Smluvními stranami elektronickým podpisem s tím, že zároveň Objednatel obdrží 1 (jeden) stejnopis s platností originálu podepsaný oběma Smluvními stranami vlastnoručně a Dodavatel obdrží 1 (jeden) stejnopis s platností originálu podepsaný oběma Smluvními stranami vlastnoručně, tj. ne elektronicky.

4.4. Nedílnou součástí této Smlouvy jsou následující přílohy:

Příloha č. 1 – „Specifikace předmětu plnění A1“
Příloha č. 2 – „Rozpočet ceny A1“

V …….. dne …….

Objednatel:

……..
Ministerstvo vnitra – Česká republika
Zástupce: plk. Mgr. Pavel Osvald

Mgr. Pavel Osvald
Digitálně podepsal Mgr. Pavel Osvald
Datum: 2021.12.30 12:15:05 +01'00'

V …….. dne …….

Dodavatel:

……..
Be a Future s.r.o.
[redacted]

[redacted]

Plnění A1 – Technická podpora a provoz MBP (fixní)

Předmětem plnění A1 jsou služby potřebné pro zajištění bezproblémového běhu Systému MBP.

Plnění bude objednáváno samostatnou Prováděcí smlouvou.

Popis jednotlivých dílčích služeb a činnosti poskytovaných v rámci Plnění A1:

Poskytování technické podpory provozu systému MBP

Zahrnuje všechny služby potřebné pro bezchybný běžný provoz systému MBP po skončení záruční doby. Hlavní úlohou je zajištění bezvýpadkového provozu systému, realizace proaktivních činností, kterými by se mělo výpadkům předcházet a v případě výpadku uvedení systému do provozního stavu.

Součástí podpory je udržování vývojového prostředí systému MBP v aktualizovaném stavu. Aktualizované vývojové prostředí bude předáno Zadavateli s ukončením Prováděcí smlouvy, která v něm vyvolala změnu.

Na všechny použité klíčové technologie (např. operační systémy, databáze, datové sklady, workflow, ESB, resp. technologie nahrazující v dodaném řešení vyjmenované) musí být zajištěna podpora výrobce po celou dobu Technické podpory.

Součástí služeb je garance funkčnosti se spolehlivostí provozu systému 99,45%, garance doby opravy 12h a prodloužená záruka – tedy služby nutné pro zajištění funkčnosti všech aplikací a modulů v případě změn rozhraní na externí systémy. Garancí funkčnosti se spolehlivostí provozu systému 99,45% je myšlena skutečnost, že Dodavatel musí zajistit dostupnost systému na úrovni 99,45%, tzn. maximální doba nedostupnosti, čímž je myšlena nahlášená a neodstraněná Vada A, nesmí překročit 0,55% doby, kdy je systém provozován (doba Zadavatelem naplánované odstávky se do doby nedostupnosti nepočítají). V případě, že nebyl funkční Service Desk a nebyl zajištěn náhradní způsob hlášení závad, doba nedostupnosti se počítá od okamžiku vzniku vady.

Incidenty nebo problémy způsobené nefunkčností nebo nedostupností MBP zaviněné Policií ČR nebo třetími osobami na straně Police ČR, např. nedodržením postupů dle příslušné provozní a administrátorské dokumentace, nejsou započítávány do doby provozování systému a nesleduje se během nich dostupnost systému pro potřeby SLA.

Požadovaná dostupnost služby 99,45% se vyhodnocuje každé fakturační období – tj, každé celé 3 měsíce od počátku poskytování služby (například za 11.8.2020 – 10.11.2020 a následně za 11.11.2020-10.2.2021).

Seznam požadovaných činností (obecný):

- Provoz Service Desku (SPoC)
- Reakce na nahlášené chyby, problémy a požadavky
- Analytická podpora řešení problémů zadaných do Service Desku
- Oprava chyb, identifikace a analýza mimořádných stavů systému
- Reakce na dotazy oprávněných uživatelů a Zadavatele
- Kontrola konzistence databází a číselníků
- Ladění výkonnosti
- Udržování testovacích databází
- Monitoring preventivní, sledování trendů, plánování změn

- Optimalizace úložišť
- Údržba a optimalizace kódu
- Kontroly provozních logů
- Kontroly integrity nastavení databáze
- Plánování výpadků systému
- Obnova provozu systému po výpadcích
- Řízení procesu eskalace mimořádných stavů a spolupráce s ostatními dodavateli na jejich řešení
- Kontrola infrastruktury a jejího nastavení
- Plánování a instalace oprav a nových verzí SW produktů, které jsou součástí systému, které jsou vyžadovány pro zajištění bezpečnosti systému nebo rozvojových aktivit, včetně zajištění funkčnosti celého sytému po provedeném upgradu
- PM, koordinace, administrativa, aktualizace dokumentace
- Prvotní zjištění a zkoumání případných změn rozhraní
- Prvotní zjištění a zkoumání nahlášených vad a stanovení návrhu řešení
- Ostatní nevyjmenované práce nutné pro garantování funkčnosti systému

Pro účely splnění požadavků Objednavatele, v souvislosti s podporou MBP, musí Dodavatel zajistit dostupnost zejména těchto specialistů:

- Projektový manažer
- Systémový architekt
- Analytik ESB
- Bezpečnostní expert
- Analytik mobilních aplikací
- Specialista pro databázi MicroFocus Vertica
- Analytik lokalizačních služeb
- Konzultant zajištění provozu
- Vývojář .Net
- Vývojář Java
- Senior specialista mobilních aplikací a jejich integrace
- Specialista inspekčních systémů elektronických dokladů
- Vývojář – Senior specialista vývoje nativních aplikací v OS Google Android
- Vývojář – Specialista vývoje nativních aplikací Apple iOS
- Vývojář – Specialista vývoje HTML/CSS/JS aplikací pro mobilní datové terminály
- Analytik MDM
- Vývojář JavaScript

- Specialista pro systém PosgreSQL
- Specialista pro systém Zabbix
- Specialista pro operační systém CentOS
- Specialista pro operační systém MS Windows Server

Zajištění podpory provozu použitých technologií

V dokumentu „popis současného stavu“ je v bodu č. 2 uvedena tabulka s přehledem použitých technologických komponent.

U všech těchto komponent musí dodavatel zajistit jejich správu (včetně přístupu ke znalostní bázi výrobců) a podporu pracovníky, kteří budou disponovat expertní znalostí jednotlivých technologických komponent. Jejich provoz je jedním ze základních požadavků objednavatele v oblasti podpory MBP.

Vyvinuté komponenty jsou instalovány jako vysoce dostupné za použití technologií high availability – jak v rámci primární lokality, tak mezi primární a záložní lokalitou.

Nad rámec uvedeného přehledu komponent, musí pracovníci Dodavatele disponovat rovněž znalostí následujících oblastí:

- Active directory
- GIS
- Informační systémy a registry státní správy (eGovernmentu), včetně využívání komunikačního rozhraní
- Radiokomunikační síť PEGAS

Dodavatel dále musí zajistit poskytování podpory výrobce následujících technologií:

FortiClient	https://www.forticlient.com/	1 ks
HP SiteScope	http://www8.hp.com/us/en/software-solutions/sitescope-application-monitoring/	1 ks
MicroFocus Service Virtualization	https://www.microfocus.com/en-us/products/service-virtualization	1 Ks
MicroFocus Vertica	https://www.vertica.com/	3 ks
Mobility Klient	http://www.urc-systems.cz/	20 Ks
Mobility Man	http://www.urc-systems.cz/	multilicence
Mobility Server	http://www.urc-systems.cz/	4 ks
PTX Mobile Kit	http://www.pointx.cz/	multilicence
ShapeX konvertor	http://www.pointx.cz/	multilicence
TeamX	http://www.pointx.cz/	multilicence
eISY - Biometrická lustrační brána	http://www.pointx.cz/	multilicence
eISY - Modul face recognition (easyGO Bioserver)	https://www.secunet.com/	1 ks

eISY – Modul klientské části komplexního inspekčního systému pro OS Windows 10 a OS Android	http://www.pointx.cz/	multilicence
eISY - Systém řízení inspekce e-dokladu u eISY/TCC	https://www.secunet.com/	1 ks záložní/ 1 ks lokalita
CMP GIS – DesktopSW - klient velitele TKS	http://www.pointx.cz/	multilicence
CMP GIS - GeoServer	http://www.pointx.cz/	multilicence
CMP GIS - Mobix Server	http://www.pointx.cz/	multilicence
CMP GIS - PTX Mobile Kit	http://www.pointx.cz/	multilicence

Poskytováním podpory výrobce je myšleno zajištění práva instalovat opravné patche i nové verze produktů a přístupu k nim.

Pro vyloučení pochybností Zadavatel uvádí, že si sám zajistí přístup k patchům a novým verzím infrastrukturního SW MS SQL serveru, MS Windows serveru a VMware vSphere.

Detailní popis podpory provozu vybraných technologií

Pro zajištění podpory provozu jednotlivých technologií, které jsou součástí MBP, bude nutné průběžně vykonávat dále uvedené činnosti. Tyto činnosti jsou upřesněním a konkretizací procesů uvedených výše v kapitole Globální řízení podpory s odkazem na metodiku ITIL. O všech činnostech musí být vedena průběžná podrobná evidence a jejich přehledná dokumentace bude také součástí pravidelného reportingu.

1 Správa událostí APV (Applications Event Management)

Procesy odpovědné za správu událostí (změny stavu, které jsou významné z hlediska řízení konfiguračních položek nebo služeb IT) během jejich životního cyklu. Důraz musí být kladen mimo jiné na následující činnosti, jejichž realizaci musí Dodavatel zajistit:

- zajištění detekce
    - událostí spojených s příjmem zpráv z mobilních telefonů;
    - událostí spojených s jejich zpracováním;
    - událostí spojených s vysokou dostupností – jak v rámci lokality (např. přepnutí clusteru), tak mezi jednotlivými lokalitami (např. výpadek komunikace);
    - událostí spojených se vstupem informací o polohách SaP;
    - typicky jsou to například (nejedná se o konečný výčet):
        - příjem neočekávané zprávy,
        - detekce neočekávaného jednání (např. přihlášení uživatele na více zařízeních),
        - nedostupnost systémů (např. Active Directory, interní systémy jako je Active Directory, MDM, GIS, atd.),
        - technické problémy (neočekávaný záznam v logu),
        - nečekaná odpověď systému,
        - problémy se systémovými prostředky (paměť, diskový prostor, otevřená spojení, souborové deskriptory apod.),
        - nestandardní stavy v databázi (např. nesprávný stav certifikátu),
        - neproběhnutí některých plánovaných úloh;
    - vstupem jsou ale také události spojené s dlouhotrvajícími procesy – např. dosažení různých sledovaných limitů, neočekávané výkyvy v reakcích systému (identifikované pomocí dostupných nebo dle potřeby zřizovaných monitorovacích nástrojů, reportů a pravidelného monitoringu jednotlivých technických a programových komponent);

- jako jeden ze vstupů slouží dále informace týkající se uvolněných patchů a verzí všech komponent APV (viz Popis prostředí);
    - Dodavatel odpovídá za aktivní monitoring a analýzu aktuálnosti softwarových součástí MBP a souvisejícího software, např. uvolněné patche a verze, prováděných minimálně jednou týdně,
    - Dodavatel dále odpovídá za monitoring aktuálnosti, funkčnosti a kompatibility aplikací a operačních systémů určených pro běh mobilních zařízení (Android, iOS, Windows) po dobu celého trvání smlouvy. Kromě obecně známých zdrojů je Dodavatel povinen zajistit si informace o existenci aktualizací softwaru a přístup k nim, např. uvolnění patche nebo verze komponent APV od Dodavatelů, kteří poskytují tyto informace pouze partnerům či jinak certifikovaným organizacím,
    - Dodavatel odpovídá, v souladu s výše uvedeným, za udržování softwarových součástí MBP a souvisejícího software v aktuálním stavu;
- jedním ze vstupů jsou také informace o změnách napojených systémů – např. Active Directory, MDM, GIS, atd.;
- vstupem jsou také doporučení bezpečnostních organizací (jako je NÚKIB, bugtraq, Microsoft, SOPHOS) – zde se předpokládá denní monitoring;

- realizace filtrace událostí
    - podpora systému, který sám rozhodne, jaká bude reakce na danou událost;
    - výstupem je záznam o události s odpovídající akcí;
    - u vybraných událostí se očekává automatizovaná reakce (např. restart dané služby se sledováním reakcí systému);
    - u událostí spojených s patchem nebo bezpečnostním doporučením je nutné definovat úvodní návrh časování implementace spolu se zahájením odpovídajícího procesu v rámci správy změn APV;

- korelace událostí
    - sledování korelace událostí a zajištění odpovídajících akcí;
    - jedná se minimálně např. o korelace:
        - událostí přímo z mobilního telefonu,
        - systému zajišťujících jejich napojení (UZK),
        - systémů realizujících jejich procesování (zbytek systémů PMS),
        - systémů PČR;

  touto činností je možné odhalit například pokusy o souběžné přihlášení nebo chyby v přiřazení uživatelů do skupin v Active Directory;

- zajištění automatické reakce
    - podle typu události je nutné zajistit adekvátní reakci – typicky notifikování odpovídající skupiny řešitelů nebo spuštění opravného programu;
    - v závislosti na typu události rozšiřovat počet automaticky řešených událostí – např. restartem služeb, změnou pravidel nebo intervalem časování úloh;

- odeslání výstrahy na základě události
    - zajištění odeslání výstrahy skupině nebo jedinci odpovědnému za řešení dané události;
    - výstraha bude typicky odeslána pomocí mailu nebo SNMP trapu;
    - příkladem události je např. počet otevřených spojení do databáze, počet obsazeného místa, počet zbývajících souborových deskriptorů nebo počet nevyřízených žádostí o certifikát;

- zajištění logování události
    - všechny detekované události musí být odpovídajícím způsobem (za pomoci stávajícího systému pro logování) zaznamenány;
    - je nutné zajistit jejich centralizaci, tak jak to umožňuje stávající systém;
- reakce administrátora
    - podle typu události je nutné zajistit řešení administrátorem včetně zpracování reportu o události;
    - kromě administrátorských operací (např. uvolnění místa, kontrola dostupnosti služeb) se jedná i o zahájení analýzy, zda nejde o chybu v dodávaném APV a zajištění předání zjištěných dat odpovědným osobám k řešení (pokud je daná část v záruce) nebo o aktivní iniciaci interního řešení;
- kontrola reakcí na události
    - minimálně 1x týdně provést kontrolu všech důležitých událostí a výjimek ze všech komponent APV a zkontrolovat jejich řešení.

2 Správa incidentů APV (Applications Incident Management)

Procesy odpovědné za správu životního cyklu všech incidentů. Správa incidentů zajišťuje, aby byl normální provoz služby obnoven tak rychle, jak je to možné, a aby byl minimalizován dopad na PČR. Důraz je kladen mimo jiné na následující aktivity, jejichž realizaci musí Dodavatel zajistit:

- reportování odhalených incidentů
    - jedná se jak o aplikační, tak infrastrukturní incidenty. Jejich zdrojem mohou např. být:
        - uživatelé,
        - Zabbix,
        - GrayLog,
        - vCenter,
        - konsolidované logy,
        - logy jednotlivých částí APV a to včetně logů ESB a logů z mobilních telefonů;
    - odhalený incident je nutné bez zbytečného odkladu zadat do Service Desku a zajistit obnovu služby;
- diagnóza a řešení incidentů
    - incident musí být vyřešen v souladu se zadanými SLA s cílem co nejrychleji obnovit službu;
    - součástí je odhalení všech symptomů incidentu ze všech komponent APV (s ohledem na využití unikátního ID zpráv je nutné dohledat detaily procesu nejen v centrálních lozích, ale také na jednotlivých serverech, kde jsou dostupné další detaily podle aktuální úrovně logování);
    - v případě, že je incident způsoben externími systémy (např. komunikace přes ESB), je nutné zajistit řešení tohoto incidentu ve spolupráci s odpovídajícím gestorem. V tomto případě je nutné připravit jasnou evidenci, proč a jak k dané chybě dochází, aby nebylo pochyb o tom, který externí systém je odpovědný za daný incident;
    - v případě chyby dat je nutné zajistit celkovou datovou integritu a ve spolupráci s PČR provést korektní akce nad veškerou udržovanou bází dat (viz Popis prostředí);
    - v případě vzniku situace zadávání chybných dat, která povedou k dalším chybám v systému, je nutné odstavit části APV tak, aby byla zachována funkcionalita nedotčených komponent;
    - u infrastrukturního incidentu bude řešení realizováno ve spolupráci s PČR a zároveň zajištěna migrace APV na jiné prostředky, ať již v rámci infrastrukturních komponent MBP nebo na další prostředky PČR. V případě vzniku incidentu zajistí Dodavatel

vhodnou změnou konfigurace fungování služby buď v omezeném rozsahu, nebo pro omezenou skupinu uživatelů;
- pokud to situace vyžaduje, provede Dodavatel kroky potřebné pro přepnutí do záložní lokality a pak zajištění přepnutí zpět (včetně zajištění datové integrity);
- pro plánované úlohy zajistit znovu opakování (podle povahy úlohy, pokud by při jejím opakování nedošlo např. k nekonzistenci dat);
- při vzniku incidentu Dodavatel neprodleně ověří, zda tento není řešen poskytovatelem užívaného či souvisejícího software a následně zajistí aplikaci řešení nebo aplikaci naplánuje v nejkratším možném čase. (viz Příloha č. 4 – Popis současného stavu, dále jen „Popis prostředí“);
- součástí je také implementace náhradního nebo permanentního řešení dle dohody s Objednavatelem (samozřejmě za dodržení postupů, testování v neprodukčním prostředí atd.);
- výsledný report o incidentu musí obsahovat předpokládané příčiny a návrhy pro další analýzu;
- Dodavatel zajistí odpovídající možnosti eskalace a to včetně post eskalační revize (proč bylo nutné eskalovat, poučení);
- v případě problémů většího rozsahu nebo trvajících delší dobu zajistí Dodavatel informovanost všech dotčených uživatelů (u obecné nedostupnosti zaslání informace přímo na jejich mobilní zařízení).

3 Správa problémů APV (Applications Problem Management)

Procesy odpovědné za správu všech problémů po dobu jejich celého životního cyklu. Správa problémů proaktivně zamezuje výskytu incidentů a minimalizuje dopad incidentů, kterým nemohlo být zabráněno. Důraz je kladen mimo jiné na následující aktivity, jejichž realizaci musí Dodavatel zajistit:

- identifikace problému
  - zjistit identifikaci problémů ze všech zdrojů – tedy např. na základě událostí a incidentů, či na základě jejich trendu. Součástí je také analýza aplikačních dat na problémové oblasti (jedná se např. o sledování počtu chyb při aktivitách uživatelů, počet revokovaných certifikátů, počet nerealizovaných žádostí o certifikát, počet přihlášení v čase atd.);
  - vstupem jsou také release notes komponent APV, které je nutné analyzovat a zjišťovat známé chyby a analýza znalostní báze (např. dokumentace, wiki a diskuze uživatelů);
  - identifikace problémů bude probíhat minimálně 1x týdně;
- další aktivity
  - příprava podkladů pro předání problému dalším stranám, včetně dat (viz Popis prostředí);
  - v případě vzniku potřeby na straně Objednavatele uplatnit záruky, ať přímo vůči Dodavateli, či vůči jinému poskytovateli prostředí, komponent či služeb MBP, je nutná příprava:
    - evidence proč je daný problém nárokován jako chyba v rámci záruky,
    - dat pro simulování problému;
  - součástí je také sledování řešení problému třetí stranou a poté iniciace nasazení opravy;
  - samozřejmostí je aktualizace a udržování znalostní báze a evidence známých chyb a jejich řešení;
  - součástí je také iniciace procesu Správy změn podle potřeb řešení.

4 Správa prostředí MBP (Environment Management)

Procesy odpovědné za správu všech prostředí MBP po dobu jejich celého životního cyklu. Cílem je udržování a aktualizace stávajících prostředí a tvorba nových na žádost. Důraz je kladen mimo jiné na následující aktivity, jejichž realizaci musí Dodavatel zajistit:

- udržování prostředí
    - udržování prostředí MBP, tak aby plnilo požadované úkoly a nedocházelo ke zbytečnému plýtvání prostředky (např. školicí prostředí je dostupné podle potřeb);
    - kromě dvou produkčních prostředí a produkčního prostředí pro přístup z internetu se jedná o vývojové, testovací, školící a další vytvořená prostředí podle potřeb;
    - součástí je také úprava skriptů a monitorovacích nástrojů podle požadavků na prostředí;
    - v rámci udržování prostředí je nutné zajistit i aktualizaci nástrojů sloužících k realizaci těchto prostředí, aktualizací virtualizačních nástrojů nebo nástrojů pro jejich správu;
- tvorba prostředí
    - na základě požadavku PČR vytvořit nové prostředí (např. nové školicí nebo další testovací prostředí);
    - pro toto prostředí navrhnout potřeby infrastruktury a ty zajistit buď ze zdrojů dedikovaných pro MBP nebo ve spolupráci s PČR zajistit připojení dalších zdrojů;
    - zajistit instalaci prostředí, a to včetně konfigurace a přenosu dat z jiných prostředí;
    - zajistit tvorbu dat pro potřeby užití (např. pro potřeby testování nasimulovat požadovaný stav data konfigurace, a to včetně vysoké dostupnosti);
    - součástí tvorby je také kontrola nasazení formou checklistů;
- řízený upgrade komponent
    - podle potřeb řešení zajistit koordinovaný upgrade komponent, jejich testování a nasazení ve všech dotčených prostředích;
    - počet takovýchto upgrade bude řízen podle počtu nasazovaných upgrade jednotlivých komponent;
    - pro každou novou verzi (určenou k nasazení) je nutné definovat plán upgradu podle potřeb;
    - v závislosti na typu a rozsahu upgrade je nutné zajistit obnovení (i s konverzí) dat a konfigurací.

5 Monitorování APV (Monitor Systém Operations)

Opakované sledování konfiguračních položek, služeb IT a procesů za účelem zjišťování událostí a odchylek aktuálního stavu od plánovaného stavu. Důraz je kladen mimo jiné na následující aktivity, jejichž realizaci musí Dodavatel zajistit:

- monitoring aplikace
    - sledování funkce, doby odezev, zatížení a dalších výkonnostních ukazatelů aplikace – minimálně je nutné sledovat počet chyb, průměrnou dobu odezvy lustrací a přihlášení uživatele, požadavek na sledování dalších ukazatelů může být definován přímo Objednavatelem anebo může vyplynout z vlastní činnosti Dodavatele;
    - všechny části aplikace je nutné monitorovat pomocí automatických a pravidelných manuálních testů (minimálně denně nebo týdně, frekvence a načasování bude stanoveno Objednavatelem – podle sensitivnosti kontrolované funkcionality;
    - součástí je také kontrola, že úlohy probíhají tak, jak byly naplánovány;
    - kontrola konzistence dat – podle potřeb, minimálně 1x týdně provést kontrolu konzistence dat (minimálně např. stav certifikátů v obrazu databáze a v certifikační autoritě, statistiky přihlášení včetně data posledního přihlášení, evidované výjimky

mobilů mimo MDM, uživatelé a skupiny s nastavením již neexistující v Active Directory – výčet nemusí být kompletní a může být upraven Objednavatelem);

- monitoring komponent APV
    - kontrola stavu a doby odezev jednotlivých infrastrukturních částí řešení – jako jsou databáze, aplikační servery a další komponenty (viz Popis prostředí);
- sledování dostupnosti a kapacit
    - proaktivní monitoring dostupnosti a kapacit jednotlivých komponent řešení včetně návrhu vylepšení a opravných akcí – minimálně 1x týdně;
- sledování výkonnosti aplikace
    - denní sledování dostupnosti a výkonnosti aplikace pomocí monitorovacích nástrojů, sledováním notifikací a za pomoci reportů;
- zajištění sběru monitorovací dat
    - zajištění, kontrola a realizace opravných akcí tak, aby byla požadovaná data pro metriky dostupná v odpovídající kvalitě;
    - součástí je také tvorba nových ukazatelů podle potřeb monitoringu přes SNMPv3 – nových ukazatelů se očekává v řádech jednotek měsíčně;
    - pro nové i stávající ukazatele je nutné vytvořit odpovídající reporty a nastavit limity pro odeslání událostí.

6 Správa provozu APV (Operations Management)

Funkce používaná poskytovatelem služeb IT, která provádí denní činnosti potřebné pro správu služeb IT a pro podporu infrastruktury IT. Správa provozu IT zahrnuje řízení provozu IT a správu zařízení. Tato funkce je také vykonávána PČR na úrovni infrastruktury, nicméně z pohledu MBP je nutné zajistit následující aktivity, jejichž realizaci musí Dodavatel zajistit:

- reakce na poruchy – např. u HW poruchy poskytnout podporu řešení (přesunout výkon na další servery, pomocí konfigurace omezit dodávané služby, připojit další zdroje do platformy apod.);
- reakce na infrastrukturní události – vybrané události infrastrukturní povahy je nutné brát jako vstup do Správy událostí APV. Minimálně se jedná o důležité události z HW, na kterém MBP přímo běží a další, které na ni mají vliv. Rozsah vstupů a požadovaných reakcí může být Objednavatelem rozšířen dle aktuální situace;
- udržování veškeré dokumentace v aktuálním stavu a archivace;
- správa kapacitních požadavků na místo – podle potřeb zajistit rozšíření diskových kapacit platformy;
- operační administrativa
    - podle potřeb zajistit instalování nových komponent do platformy (např. servery);
    - obdobné platí pro odinstalování vadných nebo vyřazených komponent;
    - změna operačních parametrů komponent – např. zvýšení úrovně logování, změna limitů;
    - správa nástrojů pro operační administrativu – např. nástroje pro sledování logů, jejich vytěžování, databázové nástroje, různé administrační konzole atd.;
    - periodické provádění a vyhodnocování testů odolnosti proti výpadku – minimálně 1x za 6 měsíců. První vstupní měření, od nějž se bude lhůta počítat, bude provedeno na základě dohody mezi Objednavatelem a Dodavatelem, nejpozději však do jednoho kalendářního měsíce od zahájení poskytování služeb Dodavatelem. Rozhodnutí o

zvýšení frekvence měření je v gesci Objednavatele, Dodavatel může dle okolností zvýšení frekvence navrhnout;
    - periodické provádění a vyhodnocení testů, přepnutí na záložní lokalitu – minimálně 1x za 6 měsíců. První vstupní měření, od nějž se bude lhůta počítat, bude provedeno na základě dohody mezi Objednavatelem a Dodavatelem, nejpozději však do jednoho kalendářního měsíce od zahájení poskytování služeb Dodavatelem. Rozhodnutí o zvýšení frekvence měření je v gesci Objednavatele, Dodavatel může dle okolností zvýšení frekvence navrhnout;
    - Housekeeping a preventivní údržba – např. mazání dočasných soborů, log souborů nebo odmazání dočasných dat z databází - minimálně 1x měsíčně na všech komponentách APV;

- správa operační bezpečnosti – viz následující kapitola;
- řízení zálohování, obnovy a archivace
    - po dohodě s Objednavatelem stanovit a zajistit odpovídající strategii zálohování a obnovy podle aktuálních potřeb a její realizaci. Strategie musí mít podobu dokumentu odsouhlaseného Objednavatelem. Dodavatel odpovídá za aktuálnost související dokumentace;
    - pravidelné ověřování zálohovaných dat – minimálně 1x za 2 měsíce;
    - podle potřeb zajistit obnovu dat;
    - po dohodě s Objednavatelem stanovit a zajistit odpovídající strategii archivace podle aktuálních potřeb a zajistit její realizaci. Strategie musí mít podobu dokumentu odsouhlaseného Objednavatelem. Dodavatel odpovídá za aktuálnost související dokumentace;
- správa vysoké dostupnosti
    - zajistit funkčnost komponent vysoké dostupnosti řešení;
    - průběžně monitorovat stav a připravenost systému k přepnutí do záložní lokality;
    - minimálně jednou ročně naplánovat a realizovat test výpadku primární lokality a následně obnovu provozu.

ZAJIŠTĚNÍ A PODPORA BEZPEČNOSTI

Bezpečnost provozu Mobilní bezpečné platformy Policie České republiky (dále jen „MBP“) bude zajišťována nejen prostředky platformy samotné, ale také bezpečnostními správci jak na straně dodavatele, tak i na straně objednavatele, jejichž vzájemná kooperace bude nezbytná. Pro účely správy bezpečnosti systémů tvořících MBP jsou definovány okruhy činností, které musí být těmito správci v rámci servisní podpory provozu MBP zajišťovány. Jedná se zejména o:

- Provoz bezpečnosti MBP
    - pravidelný monitoring definovaných služeb včetně kontroly logů v informačním systému – minimálně 1x týdně;
    - sledování dodržování bezpečnostních politik a nastavených metrik;
    - identifikace a hlášení bezpečnostních incidentů;
    - zpracování běžné agendy spojené s procesem řízení bezpečnostních incidentů;
    - eskalace incidentů;
    - využití řešení pro zjišťování „anomálií“ a ticketing;
    - pravidelné vyhodnocování operačních kontrol;
    - návrh na optimalizace nebo aktualizace bezpečnostních parametrů (jako reakce na provedené kontroly a zjištění).
- Analýza a řízení bezpečnosti, incidentů a událostí MBP

- analýza bezpečnostních incidentů a podkladů od operátorů provozu MBP – minimálně 1x měsíčně;
- návrh protiopatření bezpečnostních incidentů;
- vyhodnocování operativních návrhů od operátorů provozu bezpečnosti MBP;
- stanovení postupu pro klasifikaci informací;
- zapracování změn do dokumentace;
- návrh na reportování;
- integrace identifikace rizik, hrozeb, zranitelností a řízení do životního cyklu procesů;
- hodnocení rizik u nových souvisejících projektů nebo služeb;
- zajištění rozvoje, komunikace a údržby standardů, postupů a ostatní dokumentace (např. pokyny, směrnice, kodexy chování), které podporují zásady informační bezpečnosti;
- vytvoření eskalačních a komunikačních procesů a odpovědných rolí;
- příprava podkladů pro skupinu řízení bezpečnosti;
- tvorba reportů a poskytování informací vybraným pracovníkům;
- aktualizace bezpečnostní dokumentace a politik.

- Správa bezpečnosti MBP
  - záloha konfigurace dohledových systémů;
  - instalace kritických hotfixů a bezpečnostních upgradů (pokud budou vydány);
  - reakce na zjištěné bezpečnostní problémy v jednotlivých komponentách MBP, zejména testování a aplikace balíčků aktualizací, aplikačních pravidel;
  - kontrola a report průběžného zatížení řešení a počtu zpracovaných událostí;
  - kontrola pomocných podsystémů, archivace, notifikace, Service Desku a knowledge base;
  - optimalizace pravidel, reportů a jiných nastavení, která by mohla zatěžovat systém;
  - definice a správa rozhraní mezi jednotlivými komponentami řešení sběru a vyhodnocování bezpečnostních událostí;
  - aktualizace a optimalizace bezpečnostních parametrů platformy a jejích komponent;
  - úprava konfigurace řešení v souladu s požadavky;
  - příprava technických podkladů pro změnové požadavky;
  - spolupráce s pracovníky na řešení incidentů;
  - pravidelná administrace bezpečnostních subsystémů a kontrola řešení.

Pracovníci dodavatele, pověření odpovědností za správu bezpečnosti MBP, budou vykonávat své činnosti v souladu s interní předpisovou základnou odboru informatiky a provozu informačních technologií Policejního prezidia České republiky a budou v úzkém kontaktu s pracovníky tohoto odboru. Dodavatel bude úzce spolupracovat také s provozními správci jednotlivých monitorovaných systémů.

PODPORA ŽIVOTNÍHO CYKLU APLIKACÍ

S ohledem na rozvoj dalších aplikací využívajících MBP je nutné zajistit dodržování navržených standardů. Budoucí aplikace (ať již realizované Policií České republiky nebo třetí stranou) je nutné zařadit do platformy a odpovídajícím způsobem zajistit, že tyto nové aplikace nebudou v kolizi s již existujícími. K tomuto účelu musí být v rámci servisní podpory provozu MBP zajištěny i dále uvedené činnosti. Tyto činnosti budou vykonávány jako konzultační služby podpory na vyžádání Policie České republiky.

- Plánování kapacit

- na základě odhadů využití aplikace bude vždy nutné validovat kapacitu řešení a provést potřebná opatření nebo úpravy;
- kromě analýzy nárůstu výkonu systémů se jedná zejména o analýzu zatížení sítí, a to jako mobilních tak i rádiové sítě Tetrapol.

- Validace mobilních aplikací
  - kontrola užitých vzorů a zejména test komunikace a ukládání dat nové aplikace (zda je v souladu s bezpečností a v souladu s cíli platformy);
  - podpora pro dodávané SDK – řešení technických dotazů, pomoc při vývoji;
  - podpora při ladění a deploymentu aplikací.
- Validace bezpečnosti řešení
  - na základě specifikace aplikace bude vždy nutné provést kontrolu užitých vzorů v rámci aplikace, zda je vše v souladu s návrhem zabezpečení, a provést potřebná opatření nebo úpravy;
  - každá nová komponenta musí splňovat všechna kritéria provozu a bezpečnosti. Její začlenění nesmí snížit bezpečnost platformy.
- Validace služeb
  - dodávané služby musí splňovat standardy pro vývoj služeb a verzování a musí být nasazeny v souladu se stávajícím řešením;
  - metodická podpora při využití dodaných integračních postupů v rámci řešení ESB tj. využití stávajících integračních vzorů řešení ESB při integraci jejich aplikací;
  - kooperace při výběru správného integračního vzoru v rámci přípravy integračního řešení;
  - vytvoření simulátorů externích systémů nutných pro testování funkčnosti dalších řešení;
  - podpora pro vývojové/integrační nástroje použité v řešení služeb;
  - podpora při ladění a deploymetu projektu pro služby (např. monitoring procesů v debug módu, sledování postupu zpracování požadavků, hodnoty proměnných, krokování procesu, definice breakpoints);
  - rozšíření řešení o další typy zpráv, jejich konfigurace.
- Validace UX
  - na základě specifikace aplikace bude vždy nutné provést validaci grafického uživatelského rozhraní aplikace proti schváleným standardům a UX.
- Udržování a aktualizace komponent APV
  - průběžné udržování zdrojových kódů, tak aby byl software udržovatelný a používal aktuální verze knihoven;
  - v případě ukončení udržování externích knihoven bude zajištěna odpovídající náhrada.
- Obecná podpora při testování
- Zavedení aplikace do systému a nastavení
  - vytvoření úvodní konfigurace;
  - zavedení certifikátu aplikace do řešení;
  - kontrola navržených skupin pro konfigurační matici;
  - definice povolených komunikačních kanálů a dalších omezení.

Vlastní nasazení komponent a služeb.

Service Desk

Je požadováno, aby existovalo jednotné kontaktní místo mezi poskytovatelem služeb servisní podpory provozu MBP a jeho administrátory, případně i uživateli pro správu incidentů a požadavků, tzv. Service Desk, který bude zajišťovat procesy Request Fulfilment.

Základní funkce, které musí Service Desk pokrývat, jsou zejména:

- příjem a řízení životního cyklu všech problémů a požadavků,
- prvotní analýza problémů a požadavků a přidělování problémů a požadavků k řešení,
- řešení problémů a vybraných typů požadavků,
- monitoring a reportování stavů problémů a požadavků a plnění parametrů SLA,
- koordinace provozu MBP s provozem ostatních souvisejících informačních systémů,
- eskalace problémů na výrobce SW, který je součástí MBP,
- dokumentace problémů, příčin vzniku a jejich řešení.

Objednavatel konstatuje, že výčet základních funkcí, jež budou centrální službou Service Desk řešeny nemusí být kompletní, a může být ze strany Objednavatele průběžně požadováno rozšíření o další funkce směřující ke zkvalitnění poskytovaných služeb.

Dodavatel musí požadavek Objednavatele na rozšíření služeb poskytovaných centrální službou Service Desk splnit neprodleně, nejdéle však ve lhůtě do 10-ti dní, vyjma situace, kdy tento požadavek bude zcela zjevně nepřiměřený povaze a rozsahu služeb, které budou specifikovány uzavřenou smlouvou a jejími přílohami.

Poskytování technické podpory (pro plnění A1 i A2) pro systém eISY bude zajišťováno od ukončení smlouvy č.j. PPR-4472-20/ČJ-2018-990656 (č. smlouvy dodavatele: PČR-0103-2018), tedy ode dne 29. 6. 2021. Poskytování technické podpory (pro plnění A1 i A2) taktického koordinačního systému pro SW a HW pořízeného v projektu PDP4 bude zajišťováno od ukončení smlouvy č. j. PPR-22957-22/ČJ-2017-990656, tedy ode dne 1. 12. 2022. Tzn., že poskytování standardní výše popsanmé technické podpory (plnění A1 i A2) ze strany dodavatele bude vztahováno od uvedených datumů i pro systém eISY a pro taktický koordinační systém pro SW a HW pořízeného v projektu PDP4. Přírůstek nových technologií do MBP, který se týká systému eISY a taktického koordinačního systému pro SW a HW pořízeného v projektu PDP 4 je uveden v příloze č. 3 ZD Popis současného stavu – v části komponenty aplikačního programového vybavení.

Záruka na Plnění A1

Všechny vady, včetně záručních, jsou odstraňovány v rámci plnění A1 po celou dobu jeho poskytování.

Objednání / Akceptace plnění

Technická podpora se bude objednávat Prováděcí smlouvou a hradí se paušální platbou.

Plnění v rámci technické podpory je akceptováno na základě podpisu akceptačního protokolu. Akceptační protokol musí zejména přesně uvádět souhrn všech aktivit s členěním, jaké plnění bylo poskytnuto, kdy k plnění došlo, jak dlouho trvalo, kdo jej provedl, kdo jej zadal/převzal a kdy.

Akceptační protokoly budou podepisovány vždy za uplynulé kalendářní čtvrtletí. Ke dni podpisu akceptačního protokolu Zadavatelem nesmí být evidována žádná vada, s jejímž odstraněním by byl Dodavatel v prodlení, v takovém případě může být dílčí akceptační protokol podepsán Zadavatelem až po odstranění těchto vad. Podkladem pro fakturaci je akceptační protokol za předchozí kalendářní čtvrtletí, pokud se Smluvní strany v příslušné Prováděcí smlouvě nedohodnou jinak.

Kategorie incidentů/servisních záznamů

Za incident nebo servisní záznam je považována jakákoliv událost, která narušuje nebo by mohla narušit funkčnost dodaného plnění. Tyto události jsou reprezentovány servisním záznamem se stanovenou závažností. Za incident se nepovažuje porucha způsobená vyšší mocí, tj. živelnou pohromou, válečným konfliktem nebo teroristickým útokem anebo jinými podobnými událostmi, jež nastaly nezávisle na vůli Dodavatele a brání mu ve splnění jeho povinností, jestliže nelze rozumně předpokládat, že by Dodavatel tuto překážku nebo její následky odvrátil nebo překonal a dále, že by v době vzniku závazku tuto překážku předvídal.

Pro účely Technické podpory - Plnění A1 jsou definovány následující kategorie:

1) **kategorie A – podstatná vada (havárie)**, která

- způsobuje, že systém neposkytuje některou z kritických funkcionalit systému (systém nesplňuje účel, pro který byl vytvořen, nebo uživatelé nemohou používat všechny používané funkcionality) nebo/a zároveň,
- činí zcela nefunkčním některou z komponent systému MBP a znemožňuje provedení požadovaných akceptačních testů nebo jinou akceptační proceduru nebo/a zároveň,
- způsobuje, že systém vykazuje nepřiměřeně dlouhé odezvy nebo/a zároveň,
- způsobí nefunkční službu Service Desk, pokud není zajištěn náhradní způsob hlášení chyb

2) **kategorie B – méně závažná vada (chyba)**, která

- způsobuje, že je systém schopen omezeného provozu nebo neposkytuje některou z nekritických funkcionalit (systém splňuje účel, pro který byl vytvořen; uživatelé mohou používat všechny používané funkcionality) nebo/a zároveň;
- způsobuje, že některá z funkcionalit systému není plně činná nebo ztěžuje užívání u některého koncového uživatele, avšak tento stav má jen zanedbatelné dopady na provoz u Zadavatele nebo/a zároveň,
- způsobí nefunkční službu Service Desk, pokud je zajištěn náhradní způsob hlášení chyb.

3) **kategorie C – (nedostatek)**

- jsou ostatní vady/incidenty/požadavky, které nespadají do kategorie A ani B.

Problém:

Neznámá příčina jednoho nebo více incidentů, událost vyžadující řešení mimo rozsah událostí typu incident. Tyto události jsou reprezentovány servisním záznamem se závažností odpovídající nejvážnějšímu z incidentů.

Plánovaná odstávka – Zadavatelem schválený čas, po který nebude systém MBP dostupný v jedné nebo více svých funkcích, např. kvůli upgrade SW a nasazování nové verze.

Oprava - doba od nahlášení incidentu do vyřešení incidentu, závady, problému nebo požadavku nahlášeného formou servisního záznamu na Service Desk

Odezva – doba od nahlášení do zahájení řešení incidentu, závady, problému nebo požadavku nahlášeného formou servisního záznamu na Service Desk

Závažnost (Severity)	**Doba odezvy (Response Time)**	**Doba řešení (Fix Time)**
HAVÁRIE (A)	Do 1 hod.	Do 12 hod.
CHYBA (B)	Do 1 hod.	Do 72 hod.
NEDOSTATEK (C)	Do konce následujícího pracovního dne.	Přidělení pracovníka na řešení do 1 pracovního dne, návrh postupu řešení do 2 pracovních dnů, realizace řešení do 20 pracovních dnů, nebo dle dohody.

SANKCE pro Plnění A1

V případě nedodržení výše stanovených parametrů SLA vzniká Zadavateli nárok na smluvní pokutu v následující výši:

Překročení povolené doby nedostupnosti	**Smluvní pokuta**
Větší než 0 hodin, ale menší než nebo rovnající se 24 hodin za sledované období	100 000 Kč
Větší než 24 hodin, ale menší než nebo rovnající se 48 hodin za sledované období	300 000 Kč
Větší než 48 hodin a za každých dalších započatých 48 hodin za sledované období.	500 000 Kč

Zadavatel vyhodnotí vznik nároku na smluvní pokutu vždy do 15 dnů od konce fakturačního období poskytované služby– tj, každé celé 3 měsíce od počátku poskytování služby (například za 11.8.2020 – 10.11.2020 a následně za 11.11.2020-10.2.2021)

Výše smluvní pokuty se vyčísluje vždy s ohledem na dostupnost systému ve sledovaném období (tj. každé 3 měsíce od zahájení poskytování konkrétní služby dle příslušné Prováděcí smlouvy na technickou podporu. Pokud není v Prováděcí smlouvě uvedeno jinak, služba se poskytuje ode dne účinnosti Prováděcí smlouvy).

V případě prodlení Dodavatele s dodržením odezvy a doby opravy dle smlouvy je Dodavatel povinen uhradit Zadavateli následující smluvní pokuty:

a) kategorie A (podstatná vada)

Smluvní pokuta ve výši 1 000 Kč za každou započatou 1 hodinu překročení doby odezvy. Smluvní pokuta ve výši 2 000 Kč za každou započatou 1 hodinu překročení doby opravy.

b) kategorie B (méně závažná vada)

Smluvní pokuta ve výši 500 Kč za každou započatou 1 hodinu překročení doby odezvy. Smluvní pokuta ve výši 1 000 Kč za každých započatých 24 hodin překročení doby opravy.

c) kategorie C (nedostatek)

Smluvní pokuta ve výši 5 000 Kč za každých započatých 24 hodin překročení doby opravy.

Smluvní pokuta je splatná ve lhůtě 30 dnů od dne doručení písemné výzvy oprávněné Smluvní strany k její úhradě povinnou Smluvní stranou, není-li ve výzvě uvedena lhůta delší.

Příloha č. 2 - Specifikace ceny

Příloha č. 2 smlouvy č.j.: PPR-42481-3/ČJ-2021-990656

Plnění A1 - poskytování technické podpory provozu MBP - fixní část služeb

cena bez DPH v Kč za 2. rok plnění	cena s DPH v Kč za 2. rok plnění
17 340 000,00	20 981 400,00