Specifikace předmětu plnění - rozsah služeb

I. Plnění A – fixní služby

1. (a) Poskytování technické podpory provozu Mobilní bezpečné platformy Policie ČR – fixní část služeb

1.1. Podpora provozu technologií APV

Pro zajištění provozu systému, Service desku, proaktivního odhalování a odstraňování nedostatků a vad, garance funkčnosti, rychlé prvotní zjištění a zkoumání případných změn rozhraní, vlivů okolí apod. a pro zajištění níže uvedené SLA, rozšířených služeb nad rámec záruky (pro rychlé prvotní zjištění a zkoumání nahlášených vad a stanovení návrhu řešení) budou poskytovány následující fixní služby:

Specifikace služeb	Stanovená frekvence	Minimální počet člověkohodin v měsíci
Service Desk a Konzultační služby podpory:		
Dodavatel bude zajišťovat jednotné kontaktní místo, které bude mít formu služby Service Desk a Konzultační služby podpory. Jednotné kontaktní místo bude mít primárně podobu webové služby zřízené a provozované Dodavatelem, k níž budou určeni pracovníci Objednatele (viz Příloha č. 5) vzdáleně přistupovat přes webové rozhraní. Dodavatel zřídí určeným pracovníkům Objednatele vzdálený přístup k jednotnému kontaktnímu místu. Kromě vzdáleného přístupu zajistí Dodavatel minimálně další 2 způsoby komunikace s jednotným kontaktním místem. Dostupnost systému Service Desk bude zajištěna v režimu 24x7 za současného dodržení parametrů SLA uvedených v Příloze č. 2, čl. I bod 3. Dále bude poskytována služba Konzultační služby podpory pro zajištění reaktivních služeb podpory zaměřených na řešení problémů a závad, které nebylo možné odhalit v rámci proaktivních služeb supportu. Služba bude poskytována v režimu 5x10 (v pracovní dny v rozmezí 7:30 – 17:30 hod) za současného dodržení parametrů SLA uvedených v Příloze č. 2, čl. I bod 3. Služby Service Desk a Konzultační služby podpory budou poskytovat zejména následující funkce:	Viz popis	Viz popis

• příjem a řízení životního cyklu všech incidentů, problémů a požadavků, • prvotní analýza incidentů, problémů a požadavků a jejich přidělování k řešení, • řešení incidentů, problémů a vybraných typů požadavků, • monitoring a reportování stavů incidentů, problémů a požadavků a plnění parametrů SLA, • koordinace provozu Mobilní bezpečné platformy Policie ČR s provozem ostatních souvisejících informačních systémů, • eskalace problémů na výrobce SW, který je součástí Mobilní bezpečné platformy Policie ČR, • dokumentace incidentů, problémů, příčin vzniku a jejich řešení. Obě služby musí být schopny shora uvedené činnosti zajistit ve vztahu ke všem aktuálním funkcím MBP, jejichž rozsah se může v důsledku rozvoje MBP rozšiřovat. Dodavatel vyhotoví a předá Objednateli 1x měsíčně strukturovaný souhrnný report o stavu všech otevřených nebo v daném měsíci uzavřených incidentů, problémů a požadavků, z něhož budou zřejmé minimálně následující údaje: • předmět incidentu, problému nebo požadavku, • jejich stav, • čas nahlášení, registrace a autorizace, • doba odezvy, • doba řešení, • čas a způsob uzavření a autorizace, • doba a důvod nedostupnosti SD, • doba a důvod nedostupnosti KSP • doba a důvod nedostupnosti MBP nebo její části. Dodavatel je dále Objednateli povinen na vyžádání poskytnout ve lhůtě 10-ti dnů veškerá data služeb Service Desk a Konzultační služby podpory ve strojově zpracovatelné podobě (např. *.xml, *.csv apod.)		
Základní podpora provozu technologií (APV)		
Správa událostí APV:		
- Procesy odpovědné za správu událostí (změny stavu, které jsou významné z hlediska řízení konfiguračních položek nebo služeb IT) během jejich životního cyklu. Dodavatel je povinen zajistit zejména následující činnosti:		
1. Zajištění detekce událostí • událostí spojených s příjmem zpráv z mobilních telefonů; • událostí spojených s jejich zpracováním;	Průběžně	**80**

• 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 ISKO2, Active Directory, MDM, PATROS, SIS II, ICIS, Opatření, 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 Příloha č. 1). ▪ 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 systému 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. ISKO2, Active Directory, MDM, PATROS, SIS II, ICIS, Opatření, GIS, atd. • Vstupem jsou také doporučení bezpečnostních organizací (jako je CERT, bugtraq, SAN, SecurityFocus, X-Force, Microsoft, SOPHOS) – zde se předpokládá denní monitoring.		

2. 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.	Průběžně	
3. 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. (Díky tomu je možné odhalit například pokusy o souběžné přihlášení nebo chyby v přiřazení uživatelů do skupin v Active Directory.)	Průběžně	
4. 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. • Dle typu události je nutné zajistit adekvátní reakci automatickou nebo manuální.	Průběžně	
5. 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.)	Průběžně	
6. 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.	Průběžně	

7. Reakce administrátora • Podle typu události je nutné zajistit řešení administrátorem včetně zpracování reportu o události. • Kromě administrátorských operací 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.	Průběžně	
8. Kontrola reakcí na události • Minimálně 1x týdně provést kontrolu všech důležitých událostí a výjimek ze všech komponent APV a zkontrolovat jejich řešení.	1x týdně	
Správa incidentů APV:		
- 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 činnost Objednatele. Dodavatel je povinen zajistit zejména následující činnosti:		
1. Reportování odhalených incidentů • Jedná se jak o aplikační, tak infrastrukturní incidenty. Jejich zdrojem mohou např. být: ▪ uživatelé, ▪ HP SiteScope, ▪ cacti, ▪ Cloud System Matrix, ▪ 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.	1x týdně	**56**
2. 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.	Průběžně	

• 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. 1 – Popis prostředí, komponenty a služby, dále jen Příloha č. 1) • 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).		
Správa problémů APV:		
- 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. Dodavatel je povinen zajistit zejména následující činnosti:		
1. Identifikace problému • Zajistit 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.).	Průběžně	**32**

• 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.		
2. 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.	Průběžně	
Správa prostředí MBP:		
1. Udržování prostředí • Udržování prostředí MBP, tak aby plnilo požadované úkoly a nedocházelo ke zbytečnému plýtvání prostředky (např. školicí prostředí je dostupné podle potřeb). • Kromě produkčního prostředí se jedná o vývojové, testovací, školicí 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, počínaje aktualizací HW, aktualizací virtualizačních nástrojů nebo nástrojů pro jejich správu.	Průběžně	**40**
Monitorování APV:		
- 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:		

1. Monitoring aplikací • 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 pomoci 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.	Průběžně 1x denně Průběžně 1x týdně	**32**
2. Monitoring komponent APV • Kontrola stavu a doby odezev jednotlivých infrastrukturních částí řešení – jako jsou databáze, aplikační servery a další komponenty (viz Příloha č. 1).	1x týdně	
3. Sledování dostupnosti a kapacit • Proaktivní monitoring dostupnosti a kapacit jednotlivých komponent řešení včetně návrhu vylepšení a opravných akcí – minimálně 1x týdně.	1x týdně	
4. Sledování výkonnosti aplikace • Denní sledování dostupnosti a výkonnosti aplikace pomocí monitorovacích nástrojů, sledováním notifikací a za pomoci reportů.	Průběžně	
5. Zajištění sběru monitorovací dat • Zajištění, kontrola a realizace opravný 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.	Průběžně	

Realizace požadavků:		
- Proces odpovědný za realizaci odpovědí na otázky relevantní k APV, eskalování výsledků analýz a korektivních operací, ale také zajišťuje reportování. Důraz je kladen mimo jiné na následující aktivity, jejichž realizaci musí Dodavatel zajistit:		
• Podpora koncových uživatelů PČR, dle jejich specifických činností • Požadovaná úroveň podpory obsahuje otázky na různých úrovních složitosti. Příklady takových otázek mohou být: ▪ Vysvětlení důvodu chybového hlášení – např. co znamená „Chyba načtení konfigurace uživatele“. ▪ Vysvětlení jaké konfigurace se pro daného uživatele aplikují – jak je vlastně sestavena konfigurační matice. ▪ V jaké vrstvě a s jakými atributy musím mít uživatele X, aby viděl uživatele Y. ▪ Analýza zpoždění prováděné operace - např. u lustrací, která komponenta způsobuje jaké zpoždění. ▪ Zjištění, toku dat přes systémy – např. přes jaké služby se zaznamenává poloha konkrétního SaP. ▪ Jaká funkcionalita způsobuje největší spotřebu elektrické energie. ▪ Obecné otázky na funkcionalitu APV. ▪ Dotazy na konkrétní parametry konfigurační matice. ▪ Řešení síťových otázek – typu komunikace mezi lokalitami, připojení přes APN PČR a test dostupnosti zdrojů na obou lokalitách. ▪ Validace dat odesílaných a získávaných buď interně nebo přes ESB. ▪ Analýza toku dat přes síť Tetrapol. ▪ Výčet není kompletní, otázky budou specifikovány průběžně dle potřeby Objednavatele. • Součástí jsou také požadavky na obnovu dat a transfer dat mezi prostředími s transformací. • V případě opakujících se požadavků je nutné připravit standardizovaný postup jak takové typy požadavků řešit. • Předpokládaný počet takových žádostí je v počtu desítek měsíčně. • Podle potřeb může být požadováno i provedení pokročilých operací jako je profilování běžících aplikací, trasování běžících procesů apod. • V rámci realizace požadavků se předpokládá i dodávání reportů o běhu nebo stavu APV. Požadovány jsou minimálně následující reporty, které budou dodávány periodicky – týdně nebo podle potřeb Objednavatele): ▪ Počet aktivních uživatelů platformy, včetně rozdělení na jednotlivé kraje. ▪ Počet provedených lustrací, včetně analýzy chyb a průměrné doby odezvy. ▪ Počet provedených přihlášení, včetně analýzy chyb a průměrné doby odezvy.	Průběžně	**40**

▪ Počet provedených lustrací, včetně analýzy chyb a průměrné doby odezvy. ▪ Počet evidovaných SaP a bodů zájmu. ▪ Počet přenesených zpráv podle typu a času. Výčet a frekvence požadovaných reportů budou Objednavatelem stanovovány průběžně.		
Ostatní support (koordinace, administrativa):		
- Jedná se zejména o činnosti spojené se zajištěním součinnosti, případně i pro experty v roli konzultantů pro přijetí rozhodnutí přímo nesouvisejících s provozem MBP. Detailní forma bude přizpůsobena požadavkům vyplývajícím ze zkušeností s provozem MBP.	Průběžně	**56**

Poskytování technické podpory provozu MBP bude Dodavatelem realizováno v souladu s popsanými činnostmi, za dodržení odpovídajících procesů metodiky ITIL® 2011 Edition v následujících oblastech:

- Incident Management
- Problem Management
- Service Asset and Configuration Management
- Change Management
- Release Management
- Configuration Management

1.2. Zajištění a podpora bezpečnosti MBP

Problematika podpory a rozvoje MBP, je neoddělitelně spojena s otázkou bezpečnosti výsledných řešení, která je zajišťována jednak vlastními prostředky platformy, a zároveň i bezpečnostními správci jak na straně Dodavatele, tak i na straně Objednatele, jejichž vzájemná kooperace je nezbytná.

V souvislosti se zajištěním bezpečnosti určí Dodavatel konkrétní osoby odpovědné za správu bezpečnosti MBP.

Dodavatel je povinen při zajišťování správy bezpečnosti MBP postupovat v souladu s interními předpisy Objednatele týkajícími se zajištění bezpečnosti informačních systémů a ve spolupráci s odpovědnými pracovníky Objednatele. Dodavatel je povinen postupovat v součinnosti také s provozními správci jednotlivých monitorovaných systémů.

V případě, že dojde k rozporu mezi jednotlivými bezpečnostními správci, rozhoduje o konečném řešení Objednatel.

Dodavatel dále musí zajistit, že osoby pověřené výkonem poptávané služby v oblasti bezpečnosti, podpory provozu a rozvoje, se budou průběžně seznamovat a plně orientovat v interní předpisové základně Objednatele na úrovni a v rozsahu určeném Objednatelem tak, aby byly schopny poskytovat služby bezpečnosti, podpory provozu a rozvoje v požadovaném rozsahu a kvalitě.

Objednatel za tímto účelem zpřístupní pověřeným osobám Dodavatele potřebnou dokumentaci v rozsahu, který v souvislosti s požadovaným plněním bude nezbytný.

Pro účely správy bezpečnosti systémů tvořících MBP jsou definovány okruhy činností, které musí být těmito správci v rámci servisní podpory provozu MBP zajišťovány.

Specifikace služeb	Stanovená frekvence	Minimální počet člověkohodin v měsíci
Správa bezpečnosti MBP:		
• Pravidelný monitoring definovaných služeb včetně kontroly logů v informačním systému a případně odpovídající části SIEM.	1x týdně	**56**
• Sledování dodržování bezpečnostních politik a nastavených metrik.	Průběžně	
• Identifikace a hlášení bezpečnostních incidentů.	Průběžně	
• Zpracování běžné agendy spojené s procesem řízení bezpečnostních incidentů	Průběžně	
• Eskalace incidentů.	Průběžně	
• Využití řešení pro zjišťování „anomálií“ a ticketing.	Průběžně	
• Pravidelné vyhodnocování operačních kontrol.	1x týdně	
• Návrh na optimalizace nebo aktualizaci bezpečnostních parametrů (jako reakce na provedené kontroly a zjištění).	1x měs.	
• Záloha konfigurace dohledových systémů.	1x měs.	
• Instalace kritických hotfixů a bezpečnostních upgradů (pokud budou vydány).	Průběžně	
• Reakce na zjištěné bezpečnostní problémy v jednotlivých komponentách MBP, zejména testování a aplikace balíčků aktualizací, aplikačních pravidel.	Průběžně	
• Kontrola a report průběžného zatížení řešení a počtu zpracovaných událostí.	1x měs.	
• Kontrola pomocných podsystémů, archivace, notifikace a knowledge base.	1x měs.	
• Optimalizace pravidel, reportů a jiných nastavení, která by mohla zatěžovat systém.	Průběžně	
• Definice a správa rozhraní mezi jednotlivými komponentami řešení sběru a vyhodnocování bezpečnostních událostí.	1x měs.	
• Aktualizace a optimalizace bezpečnostních parametrů platformy a jejích komponent.	1x měs.	

• Úprava konfigurace řešení v souladu s požadavky.	Průběžně	
• Příprava technických podkladů pro změnové požadavky.	Průběžně	
• Spolupráce s pracovníky na řešení incidentů.	Průběžně	
• Pravidelná administrace bezpečnostních subsystémů a kontrola řešení.	Průběžně	

Plnění A - variabilní služby

2. (b) Poskytování technické podpory provozu Mobilní bezpečné platformy Policie ČR – variabilní část služeb (dle potřeb systému, požadavku Objednatele)

Ostatní služby pro provoz systémů a/nebo pro realizace změn, úprav systému ať již v rámci garance funkčnosti a/nebo prodloužené záruky budou poskytovány dle potřeb systémů a požadavků Objednatele. Rozsah těchto služeb je stanoven následovně s tím, že výčet je demonstrativní, závazná bude objednávka na konkrétní činnost:

2.1. Popis podpory provozu technologií APV

Specifikace služeb
Administrace serverů:
- V Příloze č. 1 Rámcové smlouvy, bod 2.1. Výčet serverů prostředí je uvedena tabulka, obsahující aktuální seznam serverů, které tvoří základ MBP, jejich operační systém a poznámku. Objednatel má právo tento seznam upravit v rámci konkrétní objednávky.
Správa prostředí MBP:
1. Tvorba prostředí • Na základě požadavku Objednatele vytvořit nové prostředí (např. nové školicí nebo další školicí 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. • V průběhu roku se předpokládá tvorba maximálně 12 nových prostředí.
2. 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.

Správa provozu APV:

- 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:

1. Správa kapacit

- řízení dostupnosti a kapacit jednotlivých komponent řešení dle návrhu vylepšení a plánu opravných akcí

2. Operační administrativa

- Podle potřeb zajistit instalování nových komponent do platformy (např. servery, síťové elementy).
- 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.
- Housekeeping a preventivní údržba - minimálně 1x měsíčně na všech komponentách APV.

3. 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 měsíčně.
- Podle potřeb zajistit obnovu dat.
- Po dohodě s Objednavatelem stanovit a zajistit odpovídající strategii archivace podle aktuálních potřeb a její realizaci. Strategie musí mít podobu dokumentu odsouhlaseného Objednavatelem. Dodavatel odpovídá za aktuálnost související dokumentace.

Podpora přechodu služeb:

- Proces realizující nerozvojové změny spojené s malým rizikem do existujícího APV a dalších komponent - změna musí být plánována, tak aby nedošlo ke kolizi s jinými změnami, v případě potřeb je nutné připravit separátní prostředí pro vývoj nebo testování dané změny, součástí je také dokumentace, plán nasazení.

Údržba APV:

- Proces realizující nerozvojové změny spojené s malým rizikem do existujícího APV a dalších ne-software komponent. Důraz je kladen mimo jiné na následující aktivity:

- Předpokládá se dodržení domluvených pravidel pro vývoj se zajištěním řízeného vývoje.
- Změny nesmí porušit práva třetích stran a nesmí dojít k porušení záruky žádné, byť jen parciální části MBP, ve vztahu k již existujícímu prostředí, komponentám a službám. (viz Příloha č. 1)
- Změna musí být plánována, tak aby nedošlo ke kolizi s jinými změnami, v případě potřeb je nutné připravit separátní prostředí pro vývoj nebo testování dané změny.
- Výsledný kód musí projít validací na bezpečnostní chyby, kontrolou popisu kódu a dodržení pravidel vývoje pro jazyk, ve kterém je změna připravena.
- Vlastníkem kódu se po jeho implementaci stává Objednavatel. Eventuální související licence ve vztahu k doprovodné dokumentaci je automaticky výhradní.
- Součástí změny je aktualizace související dokumentace, v případě potřeby Dodavatel po dohodě s Objednavatelem zajistí školení dotčených uživatelů, a to nejpozději ve lhůtě 10 dní od implementace změny.
- Pro výslednou změnu připraví Dodavatel plán nasazení a tato je zařazena do release.

Správa změn APV:

- Proces odpovědný za řízení životního cyklu všech změn APV, umožňující realizaci prospěšných změn při minimálním narušení služeb - změny musí být primárně plánované, s minimalizací doby nedostupnosti, zajištění odpovídajícího schválení změn. Každá změna bude analyzována a bude určen její dopad na prostředí a možná rizika spojená se změnou. Změnové řízení bude probíhat nejen pro interně realizované změny, ale samozřejmě také pro nasazované úpravy třetích stran. Proces odpovědný za řízení životního cyklu všech změn APV, umožňující realizaci prospěšných změn při minimálním narušení služeb IT. Důraz je kladen mimo jiné na následující aktivity, jejichž realizaci musí Dodavatel zajistit:

- Změny musí být primárně plánované, s minimalizací doby nedostupnosti.
- V případě nedostupnosti nějaké části musí být uživatel informován o stavu informační hláškou.
- U plánovaných změn je nutné informovat všechny dotčené uživatele (zaslání informace přímo na jejich mobilní zařízení).
- Samozřejmostí je zajištění odpovídajícího schválení změn Objednavatelem, avšak s umožněním realizace naléhavých změn. Realizace naléhavých změn musí být konzultována s určeným odpovědným pracovníkem Objednavatele a tímto schválena.
- Každá změna bude analyzována a bude určen její dopad na prostředí a možná rizika spojená se změnou. V případě potřeby stanovené Objednavatelem musí být výstupem analýzy dokument, který, stejně jako realizace souvisejících změn, podléhá schválení Objednavatele.
- Změnové řízení bude probíhat nejen pro interně realizované změny, ale samozřejmě také pro nasazované úpravy třetích stran - patche, nové verze nebo opravy pro části APV v záruce (viz Příloha č. 1).

Neustále zlepšování APV:

- Neustálé zlepšování služeb zajišťuje, aby služby odpovídaly měnícím se potřebám, a to tak, že se identifikují a implementují zlepšení služeb IT, která podporují požadované procesy. Cílem je zajistit mechanismus, který zajistí průběžné zlepšování APV a také zlepšování podpůrných služeb. Důraz je kladen mimo jiné na následující aktivity, jejichž realizaci musí Dodavatel zajistit:

- Pravidelná kontrola „zdraví“ komponent APV a udržování plánu rozvoje:
  - Probíhá na základě strategických cílů PČR a to minimálně čtvrtletně.
  - Obsahem je kontrola ukazatelů komponent APV jako je minimálně – průměrná doba zaučení, počet změn, délka trvání provedení jednotlivých změn, počet chyb po implementaci, počet špatně zadaných dat, náklady na podporu apod.
  - Pro definované metriky bude určeno, jak se budou měřit a jaké jsou limity.
  - Pro jednotlivé komponenty bude spravován seznam doporučených aktivit rozvoje, dále jen „akční plán“, a sledováno jeho plnění.
  - Tento plán bude realizován buď za pomoci služeb konzultační podpory přímo nebo ve spolupráci s výrobci jednotlivých komponent nebo prací s komunitou (v případě open source komponent).

Změny konfigurace APV:

- Proces zajišťující konfiguraci komponent APV (jak obecných, tak vyvinutých na míru), řízení těchto změn, validování změn konfigurace and jejich nasazení v produkci. Důraz je kladen mimo jiné na následující aktivity, jejichž realizaci musí Dodavatel zajistit:

- Analyzování dopadu konfigurační změny – např. jaký dopad bude mít změna intervalu odesílání polohy na prostředky APV včetně mobilních zařízení.
- Součástí je i vstup do plánování kapacit, např. požadavek na navýšení diskového prostoru.
- Konfigurační změny se očekávají na následujících úrovních:
  - Nastavování konfigurační matice platformy – na všech úrovních řešení, počínaje celou platformou, přes jednotlivé typy zařízení, aplikace, skupiny až po uživatelské profily.
  - Změny v plánování úloh.
  - Změny v úrovni logování částí APV.
  - Nastavení parametrů middleware, databází, ESB, messaging a v dalších komponentách APV.
  - Konfigurace pravidel přenosu pro mobilní sítě a pro rádiovou síť Tetrapol.
  - Nastavení parametrů operačních systémů – tedy Windows a Linuxu, včetně zajištění vysoké dostupnosti na úrovni clusterů, a také parametrů mobilních zařízení.
- Konfigurační změnou se rozumí také tvorba nové konfigurační entity v konfigurační matici – např. pro novou skupinu uživatelů navázanou na skupinu v Active Directory.
- Změny konfigurace musí být adekvátním způsobem validována, testována a řízeně nasazena do produkce.
- Výčet konfiguračních změn není konečný a může být ze strany Objednavatele, případně na návrh Dodavatele, průběžně doplňován a měněn dle aktuální situace.

Správa releasů a nasazení APV:

- Proces odpovědný za plánování, načasování a řízení sestavení, testování a nasazení releasů, a za implementaci této funkčnosti, přičemž chrání integritu stávajících služeb. Jako release je chápána jedna nebo více změn služby IT, které jsou sestaveny, testovány a nasazeny najednou. Jediný release může zahrnovat změny hardwaru, softwaru, dokumentace, procesů a dalších komponent. Jako nasazení (deployment) se chápe činnost, zodpovědná za nasazení nebo rozmístění nového nebo změněného hardware, software, dokumentace, procesu atd. do provozního prostředí. Důraz je kladen mimo jiné na následující aktivity, jejichž realizaci musí Dodavatel zajistit:

1. Správa release

- Release vznikají na základě analýzy požadovaných změn a podle jejich dostupnosti v čase.
- Součástí jsou vždy integrační testy napojení na ostatní systémy PČR (zejména ISKO2, Active Directory, MDM, PATROS, SIS II, ICIS, Opatření, GIS, atd.).
- Podle obsahu release je nutné připravit odpovídající Uživatelské akceptační testování, které je realizováno pomocí automatizovaných testů a manuálním testováním.
- Výstupem je plán nasazení spolu s další podpůrnou dokumentací (release notes, komunikační plán, aktualizace dokumentace) včetně její distribuce dotčeným osobám.
- Pro komponenty vyvinuté na zakázku je nutné sestavit instalační balíček a připravit odpovídající instalační skripty nebo procedury včetně odpovídající dokumentace.
- V případě změny datových formátů je nutné připravit odpovídající skripty (např. SQL) pro transformaci dat nebo připravit adekvátní manuální procedury.
- Podle povahy změn je nutné zajistit odpovídající školení.
- Samozřejmostí je rollback plán v případě problémů.

2. Nasazení

- Důraz je kladen na minimální výpadky funkčnosti MBP ve vztahu ke koncovým uživatelům.
- Po vlastním nasazení musí probíhat intenzivní monitoring řešení zejména s ohledem na stabilitu a výkon celé platformy. Je nutné počítat i s monitoringem reakce napojených systémů PČR (např. MDM, ISKO2, Active Directory) – tedy, že například nedochází k degradaci výkonu díky nevhodné formulaci dotazu, které nešlo odhalit v neprodukčním prostředí.

Správa přístupů APV:

- Proces odpovědný za to, aby uživatelé mohli používat služby IT, data nebo jiná aktiva. Správa přístupů pomáhá zajišťovat důvěrnost, důvěryhodnost, integritu a dostupnost aktiv tím, že tato aktiva mohou být modifikována pouze autorizovanými uživateli. Správa přístupů implementuje politiky správy bezpečnosti informací. Důraz je kladen mimo jiné na následující aktivity, jejichž realizaci musí Dodavatel zajistit:

- Změna přístupu je řízená a musí být zajištěno, že data jsou dostupná pouze autorizovaným uživatelům s odpovídajícími právy.
- S ohledem na možnou citlivost dat evidovaným v rámci MBP je i přístup ke čtení nutné zdůvodnit adekvátní potřebou.
- Součástí je správa přístupů k jednotlivým komponentám APV pomocí IT nástrojů.
- Předpokládaný počet takových žádostí je v počtu jednotek měsíčně.

Ostatní support (koordinace, administrativa):
- Dle žádostí Objednatele zajišťovat průběžné předávání znalostí o podporovaném APV.

2.2. Zajištění a podpora bezpečnosti MBP

S ohledem na očekávaný rozvoj dalších aplikací využívajících Mobilní bezpečnou platformu Policie ČR je nutné zajistit dodržování navržených standardů. Budoucí aplikace (ať již realizované Policií ČR 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, které budou realizovány formou variabilního plnění:

Specifikace služeb
Analýza a řízení bezpečnosti, incidentů a událostí:
• Analýza bezpečnostních incidentů a podkladů od operátorů provozu MBP – minimálně 1x měsíčně. • Návrh protiopatření bezpečnostních incidentů • Vyhodnocování operativních návrhů od operátorů bezpečnosti provozu MBP. • Stanovení postupu pro klasifikaci informací. • Zapracování změn do dokumentace. • Návrh na reportování. • Návrh na úpravu SIEM, zejména korelačních pravidel. • 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. • Generování souhrnných výstupů – grafy, dashboardy. • Aktualizace bezpečnostní dokumentace a politik.
Podpora životního cyklu aplikací:
1. 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.

2. Validace mobilních aplikací

- Kontrola užitých paternů 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.

3. 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.

4. 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 (Eclipse IDE + Apache Maven).
- 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.

5. Validace UX

- Na základě specifikace aplikace bude vždy nutné provést validaci grafického uživatelského rozhraní aplikace proti schváleným standardům a UX.

6. Obecná podpora při testování

7. 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.

3. SLA – Dohoda o požadované úrovni služeb

Dodavatel musí při poskytování Plnění A dodržovat úroveň poskytovaných služeb dle níže stanovených parametrů.

3.1. Definice použitých pojmů

SLA (Service Level Agreement) – dohoda o požadované úrovni služeb.

Service Desk – jednotné kontaktní místo, procesy a nástroje sloužící k zajištění servisní podpory a komunikaci mezi poskytovatelem servisní podpory a uživateli Mobilní bezpečné platformy Policie ČR.

Servisní podpora (Service Support) – servisní a technická činnost realizovaná Dodavatelem „na místě" i vzdáleným připojením, včetně diagnostiky a služeb Service Desk a Konzultační služby podpory, prováděná na základě servisního záznamu.

Servisní záznam (Service Ticket) – nahlášení události typu incident, problém nebo požadavek Objednatelem prostřednictvím webového rozhraní, e-mailu nebo telefonu v Service Desku. Servisní záznam může být registrován v Service Desku pouze prostřednictvím k tomu stanovených kontaktů a postupů.

Účastník veřejné zakázky uvede v Návrhu systému plnění požadavků Objednatele (Příloha B Zadávací dokumentace - Předmět a rozsah plnění veřejné zakázky, čl. 2. Obecná ustanovení) návrh postupu a kontakty pro registraci servisního záznamu.

Po registraci servisního záznamu v Service Desku musí být oprávněným zástupcem Objednatele prostřednictvím webového rozhraní vždy provedena autorizace opodstatnění k zahájení jeho řešení. Zároveň musí být servisní záznam klasifikován Objednatelem z hlediska závažnosti. O autorizaci, řešení, odmítnutí, uzavření či jiných změnách stavu a závažnosti servisního záznamu bude opět prostřednictvím webového rozhraní informován oprávněný zástupce Objednatele, kdy jednotlivá stádia, zejména pak odmítnutí a uzavření servisního záznamu, musí být Objednatelem odsouhlasena.

Závažnost (Severita) – klasifikace naléhavosti incidentu, problému nebo požadavku, která je odvozena od úrovně nefunkčnosti nebo nedostupnosti Mobilní bezpečné platformy Policie ČR.

Za dílčí vyřešení servisního záznamu pro incidenty nebo problémy se považuje i takové opatření, které způsobí změnu jeho závažnosti na nižší. Servisní záznam takto dílčím způsobem vyřešeného incidentu nebo problému má dobu vzniku shodnou se vznikem původního servisního záznamu a SLA (Response Time a Fix Time) se vztahuje na jeho aktuální závažnost.

Provozní doba (Operation Time) – doba, kdy je Mobilní bezpečná platforma Policie ČR ať již jako celek nebo její část využívána uživateli (např. 7x24 – nepřetržitá; 5x10 - v pracovních dnech 07:30 až 17:30).

Provozní doba Mobilní bezpečné platformy Policie ČR je standardně 7x24. Pro vybrané části (např. statistické funkce) může být upravena odlišně.

Plánovaná odstávka (Planned Downtime) – schválený čas, po který nebude MBP dostupná v jedné nebo více svých funkcích, např. kvůli údržbě, upgrade a testování (změnové okno). V průběhu této doby

se nepočítá Response Time a Fix Time. Plánovaná odstávka může být provedena pouze na základě předchozího souhlasu Objednatele.

Pracovní den (Working Day) – jakýkoliv den v roce mimo soboty, neděle a státem uznané svátky.

Doba odezvy (Response Time) – doba od nahlášení do zahájení řešení incidentu, problému nebo požadavku nahlášeného formou servisního záznamu.

Doba řešení (Fix Time) – doba od nahlášení do vyřešení incidentu, problému nebo požadavku nahlášeného formou servisního záznamu.

Doba dostupnosti: Doba, po níž poskytovatel služby garantuje její dostupnost.

Běžný provoz – MBP je plně dostupná ve všech svých funkcích.

3.2. Kategorizace servisních záznamů

Incident – jakákoliv událost, která narušuje, nebo by mohla narušit činnost aplikací nebo služeb Mobilní bezpečné platformy Policie ČR. Tyto události jsou reprezentovány servisním záznamem se stanovenou závažností (severitou). 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.

Závažnost (severita) může nabývat těchto stupňů (v pořadí od nejvyšší k nejnižší závažnosti):

- HAVÁRIE (kategorie A) - Mobilní bezpečná platforma Policie ČR není dostupná v jedné nebo více svých funkcích, nebo se vyskytuje funkční závada znemožňující její činnost nebo omezující běžný provoz PČR. Výčet aktuálních funkcí MBP je uveden v Příloze č. 1, kdy tento výčet se může v důsledku čl. II Plnění B této přílohy nebo vlastní rozvojovou činností Objednatele měnit.

  Za havárii se nepovažují incidenty způsobené vlivy, které nejsou objektem předmětu plnění, tj. vlivy mimo platformu MBP

- CHYBA (kategorie B) – některá z funkcí Mobilní bezpečné platformy Policie ČR nebo její část je degradována tak, že tento stav neomezuje běžný provoz MBP.

  Za chybu se nepovažují incidenty způsobené vlivy, které nejsou objektem předmětu plnění.

- NEDOSTATEK (kategorie C) – ostatní drobné incidenty, které nespadají do kategorie A nebo B.

O zařazení incidentu do jednotlivých kategorií rozhoduje odpovědný pracovník určený Objednatelem.

Problém (Problem) – 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.

Požadavek (Request) – žádost uživatele o informace, konzultační podporu, změnu apod. Specifickým typem požadavku je tzv. **Změnový požadavek** (Change Request), což je požadavek, který vyžaduje

posouzení a schválení formou standardního změnového řízení. Události kategorie požadavek jsou reprezentovány servisním záznamem se stanovením závažnosti (severity) POŽADAVEK (kategorie D).

Standardní změnové řízení – po vznesení požadavku na změnu (Change Request) musí být provedena jeho prioritizace Objednatelem, analýza rizik a přínosů, analýza dopadů na stávající konfigurační jednotky MBP, časová náročnost řešení. Analytická část bude provedena primárně Dodavatelem za poskytnutí nezbytné součinnosti Objednatele. Po provedení analýz a celkovém vyhodnocení bude Objednatelem rozhodnuto o eventuálním přijetí navrhované změny. Vlastní proces změny pak musí být proveden v souladu se standardy ITIL® 2011 Edition.

3.3. Dostupnost servisní podpory a parametry SLA

Servisní podpora bude poskytována v režimu 7x24, tedy nepřetržitě sedm dní v týdnu po dobu 24 hodin. Pro incidenty, problémy nebo požadavky nahlášené formou servisního záznamu v Service Desku platí následující parametry SLA podle stupně závažnosti. Doby odezvy a řešení se počítají od nahlášení, registrace a autorizace příslušného incidentu, problému nebo požadavku v Service Desku.

Závažnost (Severity)	**Doba odezvy (Response Time)**	**Doba řešení (Fix Time)**
HAVÁRIE (A)	Do 1 hod	Do 24 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-ti pracovních dnů, nebo dle dohody
POŽADAVEK (D)	Do konce následujícího pracovního dne.	Přidělení pracovníka na řešení do 1 pracovního dne, návrh postupu řešení do 2 pracovních dnů, realizace řešení do 20-ti pracovních dnů, nebo dle dohody

Dostupnost služeb:

Provoz MBP: dostupnost služby se stanovuje ve výši 99,5 % za fakturační období.

(Nedostupností služby je míněn stav HAVÁRIE (A), včetně havárie odstraněné v řádném termínu dle kap. 3.3, doba nedostupnosti se sčítá vždy za konkrétní fakturační období, tj. vždy za 3 měsíce poskytnutého plnění zpětně).

Service Desk (SD) a Konzultační služby podpory (KSP): dostupnost služby se stanovuje ve výši 98% za fakturační období.

3.4. Vyhodnocení dodržování SLA a penále

Dodavatel je povinen předat Objednateli reporty k ověření dodržování SLA vždy do 2 pracovních dnů od konce příslušného kalendářního měsíce. Obsah reportů je specifikován v popisu Plnění A (a). Vyhodnocení dodržení parametrů SLA za fakturované období je součástí akceptačního protokolu, který je nedílnou součástí vystavené faktury, a který musí být podepsán oběma Smluvními stranami. V případě nedodržení parametrů SLA vzniká Objednateli nárok na slevu, tak jak je určeno následovně a Dodavatel je povinen slevu zohlednit ve vystavené faktuře:

1) Nedodržení parametru dostupnost služeb:

Provoz MBP:

	Reálná dostupnost (RD)	**sleva poskytnutá Dodavatelem ve výši**
•	100% – 99,5% ……	0% z celkové ceny fixního plnění (Plnění A a)) bez DPH za daný rok dle Přílohy č. 3
•	99,5% – 0% ……..……..	(100-RD)% z celkové ceny fixního plnění (Plnění A a)) bez DPH za daný rok dle Přílohy č. 3

Reálná dostupnost 50% a níže za fakturační období, se považuje za podstatné porušení Smlouvy.

Service Desk a Konzultační služby podpory:

	Reálná dostupnost (RD)	**sleva poskytnutá Dodavatelem ve výši**
•	100% – 98% ……	0% z ceny fixního plnění za daný rok
•	98% – 0% ……..……..	(100-RD/4)% z ceny fixního plnění za daný rok

2) Nedodržení parametrů Doba odezvy a Doba řešení

Kategorie B (Chyba)

Smluvní pokuta ve výši 5000,-Kč za každých začatých 24 hodin, o které byla překročena Doba řešení a za každou hodinu překročení Doby odezvy.

Kategorie C (Nedostatek)

Doba odezvy:

- Smluvní pokuta ve výši 5000,- Kč za každých začatých 8 hodin překročení Doby odezvy.

Doba řešení:

- Smluvní pokuta ve výši 5000,- Kč za každých začatých 24 hodin překročení Doby řešení.

Kategorie D (Požadavek)

Doba odezvy:

- Smluvní pokuta ve výši 2000,- Kč za každých začatých 8 hodin překročení Doby odezvy.

Doba řešení:

- Smluvní pokuta ve výši 5000,- Kč za každých začatých 24 hodin překročení Doby řešení.

Jednotlivé slevy vzniklé ve fakturačním období se kumulují.

Maximální výše smluvní pokuty dle tohoto článku nepřekročí roční smluvní cenu za Plnění A a) bez DPH bez uplatněných slev.

II. Plnění B – Zajišťování rozvoje Mobilní bezpeční platformy Policie ČR.

Jedná se zejména o:

- tvorbu aplikací pro „Mobilní bezpečnou platformu“, plně implementovaných do stávající „Platformy mobilních zařízení“ (PMZ), s výhradním využitím „Platformy mobilních služeb“ (PMS). Implementace do stávajícího prostředí je naprosto nezbytná pro zajištění kontinuity řešení, grafického zpracování a bezpečnosti.
  - Nativní aplikace pro OS Android 5.0 a vyšší, využívající stávajícího Software development kitu (SDK).
  - Aplikace zpracované technologii HTML5 a Angular.js.
  - O zvolené technologii pro jednotlivá poptávaná řešení rozhoduje zadavatel.
- softwarový rozvoj stávajícího řešení PMZ, úpravy běhového prostředí platformy, jakož i provozovaných aplikací;
- softwarový rozvoj stávajícího řešení PMS, včetně úprav již implementované Enterprise Service Bus.