Příloha č. 2 ke Smlouvě

AZYL III

Podmínky správy a provozu

Datum aktualizace	: 31.03.2021 17:00
Počet stran	: 18

Projekt „Informační systém mezinárodní ochrany (IS AZYL III)“ (Registrační číslo: AMIF/11/01) je financován v rámci Národního programu Azylového, migračního a integračního fondu.

Obsah

Projekt „Informační systém mezinárodní ochrany (IS AZYL III)“ (Registrační číslo: AMIF/11/01) je financován v rámci Národního programu Azylového, migračního a integračního fondu.

1. Účel dokumentu

Pro informační systém IS AZYL III jsou stanoveny podmínky správy a provozu, které jsou uvedeny v tomto dokumentu. Naplnění a zachování těchto podmínek bude dále měřeno a vyhodnocováno.

Projekt „Informační systém mezinárodní ochrany (IS AZYL III)“ (Registrační číslo: AMIF/11/01) je financován v rámci Národního programu Azylového, migračního a integračního fondu.

2. Služby správy a provozu IS AZYL III

2.1. Základní požadované parametry služeb správy a provozu

Režim provozu IS AZYL III je 24 x 7
Režim podpory provozu bude 12x7 (v době pondělí až neděle v čase 8:00 – 20:00 hodin s výjimkami uvedenými v Tabulce kompetencí v kap. 2.3 tohoto dokumentu)
Požadovaná dostupnost je 99,5 % (v době pondělí až neděle v čase 8:00 – 20:00 hodin)
Maximální doba odezvy v rámci uživatelského prostředí je 5 vteřin

Dostupností se rozumí funkčnost IS AZYL III z pohledu uživatele, který tak může zpracovávat agendu související s žadateli a žádostmi o mezinárodní ochranu. Zhotovitel musí být připraven na možnou změnu režimu podpory provozu na 24x7 na výzvu Objednatele v případě vzniku krizové situace. Tato změna bude řešena samostatným dodatkem ke Smlouvě.

Výpadkem se rozumí nefunkčnost nebo omezení funkčnosti IS AZYL III, která brání uživateli zpracovávat agendu související s žadateli a žádostmi o mezinárodní ochranu. Čas výpadku se promítá negativně do dostupnosti (parametr SLA).

Za výpadek není považována:

- nedostupnost IS AZYL III v době 20:00 – 8:00 hodin,
- nedostupnost IS AZYL III v servisním okně nebo plánované odstávce,
- nedostupnost části prostředí IS AZYL III bez dopadu na uživatele,
- nedostupnost způsobená výpadkem prostředí UPAAS nebo návazných systémů (např. CIS, eSSL, RÚIAN, JIP/KAAS).

Servisní okno je čas vymezený pro provádění servisních činností, údržby, profylaxe, zálohování a dalších činností, které mohou ohrozit běžný provoz. Servisní okno pro IS AZYL III bude: každý 3. víkend v měsíci, od pátku 22.00 h do neděle 6.00 h. Bude-li z důvodu hrozící poruchy nutné tyto činnosti provádět mimo Servisní okno, musí tuto skutečnost schválit Objednatel.

Plánovaná odstávka je doba, kdy bude IS AZYL III uveden do stavu mimo provoz. Plánovaná odstávka musí být projednána a schválena Objednatelem nejméně 1 kalendářní měsíc před odstavením IS AZYL III. Do plánovaných odstávek nebo servisních oken se nepočítají časy výpadku IS AZYL III, způsobené chybou obsluhy, incidentem nebo havárií.

Projekt „Informační systém mezinárodní ochrany (IS AZYL III)“ (Registrační číslo: AMIF/11/01) je financován v rámci Národního programu Azylového, migračního a integračního fondu.

2.2. Poskytování služeb technické podpory

2.2.1. Technická podpora HW a provozního prostředí

Infrastrukturu pro IS AZYL III poskytuje Objednatel až do úrovně virtuálního prostředí, zatímco Zhotovitel odpovídá za vytvoření, správu a provoz virtuálních serverů.

2.2.2. Technická podpora a maintenance SW

Zhotovitel bude zajišťovat nákup maintenance SW produktů, které dodal v rámci veřejné zakázky s názvem „Dodávka informačního systému mezinárodní ochrany (IS AZYL III) a jeho správa, provoz a technický rozvoj" po dobu trvání smluvního vztahu. O tomto zajištění bude poskytovat Objednateli průběžné a pravidelné informace nejméně jednou ročně, jejichž součástí bude report všech licencí včetně termínů ukončení podpory a plánu nákupu prodloužení podpory.

Zhotovitel zajistí poskytování všech služeb spojených s podporou výrobce ze strany příslušného smluvního partnera (resp. vykonavatele autorských práv).

Zhotovitel je povinen do 10 dnů od dostupnosti nového změnového balíčku (opravného balíčku, aktualizace nebo nové verze SW produktu nebo OS ve virtuálním serveru) informovat Objednatele včetně analýzy dopadů instalace. Objednatel (respektive CAB – viz kapitola 2.2.5) rozhodne, jestli bude požadovat instalaci. Objednatel má právo instalaci odložit a požadovat ji kdykoliv později v průběhu Plnění. Po schválení Zhotovitelem navržených termínů ze strany Objednatele, Zhotovitel instaluje změnový balíček v termínu dle dohody s Objednatelem, nejprve na testovací prostředí, po otestování na produkční prostředí. Dle potřeby poté aktualizuje Dokumentaci (má-li instalace vliv na funkcionalitu nebo jiné parametry IS AZYL III).

Podmínky uvedené v kapitole 2.2.2. neplatí v případě SW, u kterého Objednatel využil postupu uvedeném dle článku 14. Smlouvy.

V případě, že dojde k vyčlenění některé funkcionality z produktu uvedeného v Příloze č. 4 Smlouvy, která se stane samostatným produktem nebo se stane součástí produktu jiného, bude tento produkt v rámci poskytovaných služeb poskytnut Objednateli v rozsahu užívacích práv shodném s rozsahem zakoupeným bez dalších finančních požadavků.

2.2.3. Řešení incidentů

Řešení Incidentů s garantovanou reakční dobou a maximální dobou řešení. Cílem je rychlé obnovení standardního provozního stavu a minimalizace škod výpadků. Proto je především hledán způsob, jak obnovit funkčnost postižené služby. Někdy je v rámci řešení incidentu objevena i jeho kořenová příčina, ale vždy to tak nemusí být a v tomto případě řeší kořenovou příčinu služba Řešení problémů.

Je-li to možné, je Zhotovitel povinen nabídnout Objednateli náhradní řešení. Náhradní řešení umožní uživatelům provádět požadovanou činnost náhradním, méně komfortním způsobem. Náhradní řešení musí Zhotovitel představit, Objednatel schválit a Zhotovitel aplikovat v čase „Doba zprovoznění" pro daný typ incidentu. Využití náhradního řešení může mít vliv na lhůty dané Reakční dobou a Dobou zprovoznění (Tabulka 1) tímto způsobem:

a) Objednatel může rozhodnout, že nasazením náhradního řešení došlo ke snížení kategorie incidentu, tedy lhůta pro odstranění incidentu se prodlužuje dle nižší kategorie incidentu.

b) Objednatel tímto může považovat incident za vyřešený a současně rozhodnout, že se záležitost přesouvá do služby „řešení problémů".

Při řešení Incidentů je důležité stanovení priorit, protože některé incidenty mají vyšší dopad než jiné, a proto je třeba je řešit přednostně. K tomu slouží kategorizace servisních požadavků zadávaných jako Incident v Tabulce 1:

Tabulka 1 – Řešení incidentů

Typ incidentu	Reakční doba na nahlášený incident[1]	Doba zprovoznění[2]
Kategorie III – Nefunkčnost systému jako celku nebo nefunkčnost klíčové součásti systému, eventuálně kybernetický bezpečnostní incident kategorie II či III dle níže uvedené klasifikace, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky obnovena funkčnost systému a zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.	do 2 hodin	do 8 hodin
Kategorie II – Výrazně ztěžuje nebo komplikuje činnost uživatelů IS AZYL III z důvodu selhání nebo omezení některé ze systémových funkcí	do 4 hodin	následující den

[1] Doba na reakci se počítá od nahlášení incidentu v době 8:00 – 20:00 hodin. Reakcí na nahlášený incident se rozumí započetí nápravy/opravy.

[2] V případě incidentů kategorie I a II lze pro dočasné řešení využít i způsoby, které nenaplní celkovou funkcionalitu, ale umožní uživatelům vést evidenci osob a řízení v oblasti mezinárodní ochrany v České republice (např. změna pracovního postupu, změna prostředí). Takové dočasné řešení musí Zhotovitel představit, Objednatel schválit a Zhotovitel aplikovat v čase „Doba vyřešení incidentů" pro daný typ incidentu. Využití náhradního řešení nemá vliv na lhůty dané Reakční dobou a Dobou zprovoznění, s výjimkou, kdy Kontaktní osoba Objednatele písemně potvrdí souhlas s prodloužením lhůt.

podporujících důležité procesy, eventuálně kybernetický bezpečnostní incident kategorie I dle níže uvedené klasifikace, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky obnovena funkčnost systému a zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.		
<u>Kategorie I</u> – Vyskytuje v izolované části díla nebo dílčího plnění. Využívání díla je částečně ztíženo a nemá vliv na ostatní funkce, eventuálně interní kybernetický bezpečnostní incident dle níže uvedené klasifikace, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky obnovena funkčnost systému a omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.	do 4 hodin	do 5 dnů

Projekt „Informační systém mezinárodní ochrany (IS AZYL III)“ (Registrační číslo: AMIF/11/01) je financován v rámci Národního programu Azylového, migračního a integračního fondu.

Tabulka 2 – Klasifikace kybernetických bezpečnostních incidentů:

PŘÍKLADY KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ PODLE VYHLÁŠKY O KYBERNETICKÉ BEZPEČNOSTI
upřesnění klasifikace kybernetických bezpečnostních incidentů pro Ministerstvo vnitra České republiky (v2)

Typy kybernetických bezpečnostních incidentů - PŘÍKLADY:	Kybernetická bezpečnostní událost	Interní kybernetický bezpečnostní incident - klasifikace MV	Kyberentický bezpečnostní incident - klasifikace NÚKIB		
			nízký dopad → *vysoký dopad*		
			Méně významný (Kategorie I)	Významný (Kategorie II)	Velmi významný (Kategorie III)
	nehlásí se CERT týmu	zvážit nahlášení CERT týmu	nutno hlásit CERT týmu		
neoprávněný přístup do systému / k informacím	Detekovaný nepovedený pokus o přístup do systému / k informacím (např. zapomenuté heslo).	Zneužití přístupových údajů / neoprávněný přístup k informacím zaměstnancem nebo identifikovatelnou třetí stranou. Způsobené škody jsou zanedbatelného rozsahu.	Proniknutí do systému, kde díky nastaveným oprávněním nemá útočník téměř žádné možnosti k přímému napáchání větších škod. Sběr informací o systému a prostředí. Finanční dopady menšího rozsahu (100tis.-1mil. Kč).	Proniknutí do systému, napáchání škod středního dopadu (např. narušení integrity, dostupnosti, důvěrnosti citlivých údajů). Finanční dopady středního rozsahu (1-10mil. Kč).	Získání plné kontroly nad systémem, napáchání škod velkého rozsahu (více než 10 mil. Kč). Narušení bezpečnosti systému s následkem možného ohrožení zdravía životů.
omezení dostupnosti systému / IT služeb	Plánovaná (avizovaná) nedostupnost např. z důvodu údržby nebo jakákoliv událost, jejíž opakovaný/mnohonásobný výskyt by mohl narušit dostupnost.	Krátkodobé omezení dostupnosti systému z důvodů selhání / nedostupnosti některého z podpůrných aktiv (neúmyslný provozní incident). Zpravidla se bude jednat o nedostupnost do 1hod. Výše dopadů spojená s nedostupností systému je posuzována per systém (každý	Omezení dostupnosti systému v důsledku kybernetického útoku z komunikační sítě. Nedostupnost systému do 4hod. (výše dopadů spojená s nedostupností systému je posuzována per systém). Finanční dopady menšího rozsahu (100tis.-1mil. Kč).	Omezení dostupnosti systému v důsledku kybernetického útoku z komunikační sítě. Nedostupnost systému do 24hod. (výše dopadů spojená s nedostupností systému je posuzována per systém). Finanční dopady středního rozsahu (1-10mil. Kč).	Omezení dostupnosti systému v důsledku kybernetického útoku z komunikační sítě. Déle trvající nedostupnost, obvykle více než 24 hodin (výše dopadů spojená s nedostupností systému je posuzována per systém). Finanční dopady velkého rozsahu (více než 10mil. Kč). V důsledku narušení dostupnosti systému může být ohroženo zdraví a životy občanů.
škodlivý kód	Škodlivý kód detekovaný a zachycený antivirovou ochranou dříve, než byly napáchány jakékoliv škody.	Zjištěno ojedinělé napadení systému (např. 1 stanice) známým škodlivým kódem, který byl následně úspěšně odstraněn a zároveň bylo zamezeno jeho dalšímu rozšíření.	Zjištěno napadení systému škodlivým kódem (např. více stanic/serverů), existuje podezření na kompromitaci nebo byly způsobeny škody menšího rozsahu. Finanční dopady v rozsahu 100tis.-1mil. Kč.	Zjištěno napadení systému škodlivým kódem (např. více stanic/serverů), existuje podezření na kompromitaci nebo byly způsobeny škody středního rozsahu. Finanční dopady v rozsahu 1-10mil. Kč.	Masivní napadení systému škodlivým kódem, které způsobilo škody vysokého rozsahu. Finanční dopady více než 10mil.Kč.
překonání technických opatření	Detekovaný pokus o překonání technického opatření.	Překonání technického opatření např. zneužitím zranitelnosti daného opatření, které způsobí škody zanedbatelného rozsahu.	Překonání technického opatření např. zneužitím zranitelnosti daného opatření, které způsobí škody menšího rozsahu. Finanční dopady v rozsahu 100tis.-1mil. Kč.	Překonání technického opatření např. zneužitím zranitelnosti daného opatření, které způsobí škody středního rozsahu. Finanční dopady v rozsahu 1-10mil. Kč.	Překonání technického opatření např. zneužitím zranitelnosti daného opatření, které způsobí škody vysokého rozsahu. Finanční dopady více než 10mil.Kč.
porušení organizačních opatření	Zaměstnanec se snaží např. kopírovat velké množství dat, které přímo nesouvisejí s jeho každodenní pracovní náplní, ale ke kterým potřebuje mít přístup, tato aktivita byla speciálním nástrojem detekována a zamítnuta.	Zaměstnanci např. využívají aktiva jinak než je přípustné a stanovené a tím dojde k narušení integrity nebo důvěrnosti, které způsobilo nebo může způsobit škodu zanedbatelného rozsahu.	Zaměstnanci např. využívají aktiva jinak než je přípustné a stanovené a tím dojde k narušení integrity nebo důvěrnosti, které způsobilo nebo může způsobit škodu menšího rozsahu. Finanční dopady v rozsahu 100tis.-1mil. Kč.	Zaměstnanci např. využívají aktiva jinak než je přípustné a stanovené a tím dojde k narušení integrity nebo důvěrnosti, které způsobilo nebo může způsobit škodu středního rozsahu. Finanční dopady v rozsahu 1-10mil. Kč.	Úmyslné a vědomé porušení organizačních opatření s přesahem do kyberperostoru za cílem poškodit organizaci (např. kompromitace ze strany osoby v roli administrátora) s následkem škod vysokého rozsahu. Finanční dopady více než 10mil.Kč.
sociální inženýrství, phishing	-	Neúspěšné pokusy o sociální inženýrství nebo phishing cílený na organizaci.	Dopady menšího rozsahu způsobené pomocí cíleného sociálního inženýrství nebo phishingu. Finanční dopady v rozsahu 100tis.-1mil. Kč.	Dopady středního rozsahu způsobené pomocí cíleného sociálního inženýrství nebo phishingu. Finanční dopady v rozsahu 1-10mil. Kč.	Dopady vysokého rozsahu způsobené pomocí cíleného sociálního inženýrství nebo phishingu. Finanční dopady více než 10mil.Kč.
ostatní	Jakákoliv kybernetická bezpečnostní událost, která přímo nezpůsobí incident, ale její výskyt je pro danou organizaci významný (ignorováním této události může v budoucnu dojít k incidentu).	Kybernetický bezpečnostní incident způsobující škody zanedbatelného rozsahu.	Jakýkoliv kybernetický bezpečnostní incident způsobující škody menšího rozsahu. Finanční dopady v rozsahu 100tis.-1mil. Kč.	Jakýkoliv kybernetický bezpečnostní incident způsobující škody menšího rozsahu. Finanční dopady v rozsahu 1-10mil. Kč.	Jakýkoliv kybernetický bezpečnostní incident způsobující škody menšího rozsahu. Finanční dopady více než 10mil.Kč.

Incident je řešen s prioritou odpovídající dané kategorii. Kategorie III má nejvyšší prioritu a řeší se přednostně, kategorie I má nejnižší prioritu a řeší se až po kategoriích III a II. Tyto časy mohou být prodlouženy v případě, že:

- nastala neodvratitelná událost (vyšší moc),
- nebo se vyskytly překážky na straně Objednatele nebo třetích stran, které Zhotoviteli neumožňovaly řádně poskytovat službu či ovlivnily délku nebo pracnost jednotlivých pracovních úkonů (tyto překážky musí být bezodkladně písemně nahlášeny Objednateli),
- nebo bylo řešení incidentu v konkrétním případě přerušeno s písemným souhlasem Kontaktních osob obou smluvních stran.

V průběhu řešení incidentu je Zhotovitel oprávněn požádat Objednatele o zajištění podmínek pro řádné poskytování služby, poskytnutí doplňujících informací, ověření provedeného řešení incidentu, přičemž lhůta pro odstranění incidentu se prodlužuje o tuto poskytovanou součinnost ze strany Objednatele.

Žádost o prodloužení lhůty musí Zhotovitel bez odkladu po vyskytnutí se překážky zaslat písemně Objednateli, který ji musí do následujícího dne potvrdit nebo zamítnout.

Všechny typy incidentů budou nahlášeny oprávněnou osobou Objednatele na Service Desk MV, který je zaeviduje a přepošle v podobě strukturovaného e-mailu na řešitelskou skupinu Zhotovitele dle komunikační matice připravené pro správu a provoz. Zhotovitel musí reagovat na tyto incidenty dle jejich kategorizace.

- Po prvotní analýze bude Zhotovitel informovat Service Desk MV o možných dopadech nefunkčnosti;
- Po nalezení příčiny nefunkčnosti Zhotovitel informovat Service Desk MV o pravděpodobném čase odstranění nefunkčnosti a případně alternativních způsobech řešení;
- Po odstranění nefunkčnosti bude Zhotovitel informovat Service Desk MV o způsobu vyřešení.

Práce na řešení incidentů mohou být realizovány vzdáleně pomocí přístupu VPN kanálem, nebo v nutných případech v místě provozu IS AZYL III (resp. lokalitě UPAAS). Přístup VPN má omezený čas na maximální délky spojení a není určen pro průběžný dohled (tedy není možné tuto VPN používat pro průběžný vzdálený dohled). Tento VPN přístup je na jmenné účty přidělené konkrétní osobě Zhotovitele.

Na řešení problému bude Zhotovitel pracovat až do doby, kdy bude splněno alespoň jedno z následujících kritérií:

- Vyřešení obnovení funkčnosti postižené služby v plném rozsahu.

- Informování Objednatele o tom, že nefunkčnost je způsobena z třetí stranou (vnější agendové IS, infrastruktura CMS apod.). V takovém případě Zhotovitel Objednateli poskytne součinnost při řešení této nefunkčnosti s třetí stranou.
- V případě závady produktů jiných výrobců. V takovém případě bude Zhotovitel výrobce informovat o vadě a poskytne Objednateli informace, které získal jako odpověď po eskalaci problému tomuto výrobci (s výjimkou SW produktů nakoupených a udržovaných dle článku 14 Smlouvy).

Objednatel bude Zhotovitele informovat pomocí Service Desku MV incidentech, které vzniknou v provozním prostředí UPAAS a které budou řešit správci datového centra, z důvodů předcházení důsledkům na úrovni aplikace. Stejně tak bude Objednatel Zhotovitele informovat o plánovaných servisních oknech, odstávkách a všech změnách v infrastruktuře, které by mohly mít dopad na IS AZYL III.

Práce na řešení incidentů mohou být realizovány vzdáleně pomocí přístupu VPN kanálem, nebo v nutných případech v místě provozu IS AZYL III.

2.2.4. Řešení Problémů

Tato služba probíhá na pozadí komplexu služeb zajišťujících podporu a není z pohledu Objednatele a uživatelů přímo viditelná. Předmětem služby je řešení a správa problémů v provozním prostředí.

Služba eliminuje kořenové příčiny incidentů (Problém). Cílem je zajištění maximální stability systému vyloučením možnosti znovuobjevení obdobných incidentů v budoucnu. V rámci služby vzniká databáze známých chyb včetně seznamu náhradních řešení, které umožňují rychlou obnovu funkcionality v případě incidentu.

2.2.5. Realizace změn

Předmětem služby je realizace změn v rámci IS AZYL III. Služba zahrnuje drobný rozvoj systému, stejně tak jako různé úpravy a změny v konfiguraci, jako změnové požadavky, protože prioritou je zabudovat požadovanou změnu bez rizika ohrožení chodu provozu IS AZYL III.

Poskytování této služby zaručuje Objednateli, že požadované změny budou zapracovány v dohodnutém harmonogramu a za využití počtu dohodnutých disponibilních kapacit (člověkodny) a minimalizuje rizika možného negativního vlivu změny na systém.

Před předáním IS AZYL III do provozu Zhotovitel navrhne a Objednatel reviduje a schvaluje procesy technické podpory, jejichž součástí je způsob zadávání požadavků na změnu, ustanovení a svolávání CAB (Change Advisory Board), skládající se z osob, jejichž názor je důležitý pro odhad dopadů a rizik větších a velkých změn a pro zpětné hodnocení vlivu změny na provoz, a dále pravidla pro schvalování standardních a urgentních změn.

V rámci realizace změn Zhotovitel zajistí průběžnou aktualizaci provozní, administrátorské a uživatelské dokumentace AZYL III a její zpřístupnění zástupcům Objednatele na dohodnutém úložišti tak, aby odpovídala aktuálnímu stavu implementovaného a provozovaného systému. Bude-li se měnit zdrojový kód, zaznamená rovněž změnu v něm a jednou ročně předá Zhotovitel Objednateli aktualizovaný Zdrojový kód (včetně popisu). Dokumentace musí splňovat požadavky zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů. Požadavky na dodání dokumentace vycházejí zejména z vyhlášky č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy, ve znění pozdějších předpisů, a vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Služba dále zahrnuje případné na konzultace a školení (administrátorů, uživatelů) po realizaci každé změny, kde je toto nezbytné.

Změnové požadavky mohou být vyvolány různými situacemi:

2.2.5.1. Změny vyplývající z Řešení problémů

Jestliže služba Řešení problémů identifikuje kořenovou příčinu vyvolávající Incidenty, může být nezbytné provést změny v IS AZYL III. Zhotovitel provede analýzu dopadů změny, kterou projedná v rámci v CAB (Change Advisory Board). Po odsouhlasení provede odstranění problému v IS AZYL III. Tyto opravy jsou zahrnuty v paušální platbě za Technickou podporu.

Jestliže se prokáže, že problém byl způsoben změnou nebo vadou v prostředí UPAAS nebo návazných systémů (např. CIS, eSSL, RÚIAN, JIP/KAAS), požádá Zhotovitel Objednatele o zajištění nápravy. Objednatel provede na své straně příslušná opatření, nebo objedná úpravu IS AZYL III v případě změny v UPAAS nebo návazných systémů.

2.2.5.2. Úpravy funkcionalit v IS AZYL III dle potřeby Objednatele (Drobný rozvoj)

Změnové požadavky Objednatele vyplývají:

- z požadavků Objednatele na vývoj nových nebo úpravy stávajících funkcionalit IS AZYL III,
- z organizačních nebo jiných změn na straně Objednatele, které vyžadují úpravy nastavení nebo rozšíření IS AZYL III,
- ze změn rozhraní (update, upgrade nebo jiné změny v systémech třetích stran, integrovaných nebo vyžadujících integraci se systémem IS AZYL III),
- ze změn v infrastruktuře Objednatele (změny hardware, operačních systémů, integrační vrstvy, komunikačních systémů apod., provedených na přání Objednatele a vyžadující úpravy na nich závislých částí systému IS AZYL III).

Drobný rozvoj IS AZYL III zahrnuje činnosti, které mají charakter opravy nebo údržby nehmotného majetku ve smyslu vyhlášky č. 323/2002 Sb., o rozpočtové skladbě. V těch případech, kdy by změnový požadavek objednatele měl vést k technickému zhodnocení IS AZYL III ve smyslu vyhlášky č. 323/2002 Sb., o rozpočtové skladbě, budou strany postupovat dle Přílohy č. 3 Smlouvy.

Objednatel zaeviduje požadavek na změnu a Zhotovitel připraví nabídku na realizaci změny. Tato nabídka bude obsahovat:

- popis změny – úpravy, zajišťované činnosti,
- objem práce v člověkodnech,
- harmonogram provedení,
- analýzu dopadů změny, a to zejména s ohledem na dopad na zvýšení použitelnosti IS AZYL III a případně úpravy funkcionalit IS AZYL III,
- výstupy služby, akceptační kritéria,
- platnost nabídky.

V případě, že Objednatel s nabídkou souhlasí a požaduje její realizaci, akceptuje nabídku a změna postupuje k posouzení a schválení do CAB. Po schválení zde může být realizována.

Změna je zařazena do plánu vývoje, je vyvinuta a po úspěšném testování v testovacím prostředí je se souhlasem Objednatele nasazena do produkčního prostředí. Součástí nasazení je rovněž aktualizace dokumentace a je-li to třeba, i školení klíčových uživatelů.

V případě, že Objednatel nesouhlasí s uvedenými parametry nabídky (zejména cena a harmonogram) a ani po jednání odpovědných zástupců se smluvní strany neshodnou na uvedených parametrech služby, může Odběratel vydat zamítavé stanovisko k nabídce a od konkrétního provedení služby tak odstoupit.

Předpokládaný rozsah plnění drobného rozvoje činí v průměru 8 (osm) hodin měsíčně (1 člověkoden). Realizace drobného rozvoje může být nerovnoměrně rozvržena mezi různé měsíce. Toto nerovnoměrné rozvržení nemá vliv na výši měsíční ceny, která je Objednatelem hrazena Zhotoviteli za plnění dle této přílohy Smlouvy.

2.2.5.3. Změny realizované za účelem souladu s legislativou

Objednatel požaduje po celou dobu platnosti Smlouvy, aby Zhotovitel zajišťoval soulad IS AZYL III s platnou legislativou. Zhotovitel bude povinen po celou dobu platnosti Smlouvy zajistit a garantovat chod systému i jeho dílčích modulů nebo funkcionalit tak, aby byl plně v souladu s právním řádem ČR a to včetně bezprostředně použitelných norem EU. V případě, že dojde ke změnám právních předpisů, které mohou mít vliv na zajištění souladu IS AZYL III s právní úpravou, je Zhotovitel povinen předložit Objednateli do 7 dnů od nabytí platnosti nové právní úpravy návrh úprav uživatelského prostředí zajišťujících soulad s legislativou (dále jen „Návrh úprav“) a po jeho akceptaci v CAB tyto úpravy realizuje.

Návrh úprav musí obsahovat:

a) identifikaci ustanovení právních předpisů, jejichž změna vyvolává potřeby úprav IS AZYL III a údaj o účinnosti této nové právní úpravy,
b) popis navrženého způsobu úprav IS AZYL III, jejichž prostřednictvím má být IS AZYL III uveden do souladu se změněnou právní úpravou,
c) popis dopadů změny, a to zejména s ohledem na dopad na zvýšení použitelnosti IS AZYL III a případně úpravy funkcionalit IS AZYL
d) lhůtu pro realizaci.

Do jednoho Návrhu úprav nesmí být slučovány úpravy vyvolané věcně či časově nesouvisejícími změnami právních předpisů. Zhotovitel je povinen zahájit realizaci úprav schválení v CAB. Úpravy uživatelského prostředí musí být provedeny ve lhůtě odsouhlasené Smluvními stranami v Návrhu úprav.

Postup dle této kapitoly Přílohy č. 2 Smlouvy se použije v případech, kdy zajišťování souladu IS AZYL III má charakter opravy nebo údržby nehmotného majetku ve smyslu vyhlášky č. 323/2002 Sb., o rozpočtové skladbě. Náklady na zajišťování této činnosti jsou součástí roční ceny služeb správy a provozu poskytovaných Zhotovitelem (tabulka D Přílohy č. 4 Smlouvy). V případech, kdy návrh úprav zpracovaný Zhotovitelem dle této kapitoly Přílohy č. 2 Smlouvy povede k technickému zhodnocení IS AZYL III ve smyslu vyhlášky č. 323/2002 Sb., o rozpočtové skladbě postupují strany při zajištění souladu IS AZYL III se změněnou právní úpravou podle přílohy č. 3 Smlouvy.

2.2.6. Údržba

Pravidelné provádění údržby IS AZYL III (minimálně 12× ročně) zahrnuje:

1. Vytváření pravidelných otestovaných konfiguračních záloh;
2. Kontrolu provozních systémových logů IS AZYL III případně následné řešení zjištěných problémů;
3. Pravidelný dohled nad systémovými prostředky IS AZYL III, případný návrh řešení zjištěných problémů. (Patří sem i řešení nedostatečné kapacity a výkonu HW);
4. Čištění databází;
5. Aktualizace operačních systémů a dalšího použitého SW vybavení.

2.2.7. Monitoring

Událost je změna stavu, která je významná pro službu nebo konfigurační položku. Událost může indikovat incident nebo potřebu rutinního zásahu (údržba). Jsou tedy nastavena pravidla pro výstupy z monitoringu, aby s nimi bylo zacházeno tak, aby byl systém udržován ve stabilním stavu, aby byly hrozící výpadky pokud možno eliminovány předem proaktivními zásahy, a když už k výpadku dojde, byl objeven a vyřešen co nejdříve.

Zhotovitel realizuje v rámci projektu monitorovací systém IS AZYL III a provozuje ho.

Výstupy z monitoringu aplikační části IS AZYL III, tedy funkčnosti a odezvy na uživatelské úkony (např. přihlášení), Zhotovitel analyzuje, vyhodnocuje, pro identifikované incidenty nebo problémy zakládá tickety v Service Desku MV a zajišťuje jejich řešení.

Zhotovitel bude rovněž poskytovat součinnost při změnách konfigurace monitoringu, při vyhodnocování a analýzách bezpečnostních událostí.

2.2.8. Systém zálohování a obnovy dat

Zhotovitel je odpovědný za nastavení zálohovacích úloh databáze, konfigurací a dalších dílčích částí dat AZYL III produkčního prostředí. Zhotovitel bude pravidelně ověřovat úspěšnost realizace zálohovacích úloh a řešení problémů se zálohováním. Dále bude pravidelně ověřovat funkčnost obnovených dat ze záloh.

Zhotovitel poskytne součinnosti Objednateli při řešení problémů se zálohováním virtuálních serverů prostředí IS AZYL III, které budou jako image zálohovány zálohovacím systémem UPAAS. Stejně tak poskytne součinnost v případě potřeby obnovy celého virtuálního serveru ze zálohovacího systému UPAAS.

Zhotovitel poskytne součinnosti Objednateli při realizaci DR testů a testů funkčnosti obnovy AZYL III.

2.2.9. Správa virtuálních serverů pro AZYL III

Zhotovitel zajišťuje kompletní správu všech virtuálních serverů pro AZYL III od úrovně operačního systému. Objednatel požaduje zajištění provozu a dostupnosti produkčního prostředí AZYL III dle Kapitoly 2.1 této Přílohy.

Zhotovitel zodpovídá za správu všech systémových identit, které jsou využity pro administraci prostředí AZYL III, tedy virtuálních serverů, aplikačních částí, databáze a přístupů k nim. Přehled všech používaných identit budou součástí Provozní dokumentace (bez uvedení hesel, které bude Zhotovitel uchovávat na zabezpečeném místě).

Zhotovitel bude průběžně vyhodnocovat provozní informace z pohledu dostatečné kapacity využívaného prostředí a související infrastruktury. V případě hrozby nedostatečné kapacity či výkonu využívaného prostředí a související infrastruktury poskytne Zhotovitel Objednateli tuto informaci s dostatečným předstihem, aby mohl Objednatel zajistit posílení prostředí či infrastruktury, a dále veškerou nezbytnou součinnost pro zajištění další funkčnosti IS AZYL III bez omezení nebo rizika výpadku. Tutéž součinnost poskytne Zhotovitel při dalších změnách plánovaných Objednatelem, např. při přechodu na jiný HW, jiné prostředí, výkonnější prostředí apod. Předmětem uvedené součinnosti není dodávka HW komponent. V případě změn prostředí, např. při přechodu na jiný HW, vyšší verzi operačních systémů a dalšího podpůrného

SW, zajistí Zhotovitel potřebnou součinnost (např. otestování, odladění provozních chyb na novém prostředí apod.).

2.2.10. Součinnost na ověření DR procesu

Zhotovitel poskytne na základě výzvy správců datového centra součinnost v rozsahu 20 (dvacet) hodin za rok.

2.2.11. Součinnost při plánování dalšího rozvoje

Zhotovitel poskytne součinnost při plánování dalšího rozvoje na základě výzvy v rozsahu 8 (osm) hodin za rok.

2.2.12. Reporting a akceptace služeb

Do 10 (deseti) dnů po ukončení měsíce připraví Kontaktní osoba Zhotovitele:

- Výkaz o dostupnosti IS AZYL III – výkaz bude obsahovat výčet nedostupností včetně data a přesné doby a následně výpočet celkové dostupnosti AZYL III za daný měsíc.
- Výkaz o provozních činnostech, který bude obsahovat informace o
  - Řešení incidentů – u každého incidentu bude uvedeno datum a doba vzniku incidentu a dále dodržení Reakční doby a Doby vyřešení. Rovněž bude uvedena příčina a způsob vyřešení incidentu.
  - Řešení problémů – seznam řešených problémů, termín nasazení opravy.
- Výkaz o čerpání služeb Úpravy funkcionalit v IS AZYL III dle potřeby Objednatele (Drobný rozvoj) – výkaz bude obsahovat informace o čerpání disponibilních kapacit dle kapitoly 2.2.5.2 tohoto dokumentu za reportovaný měsíc.

Výkazy poskytne Kontaktní osobě Objednatele na pravidelné schůzce, na které budou hodnoceny kvality poskytovaných služeb a jejich kontinuální zlepšování.

Informace z výše uvedených výkazů mohou být Dodavatelem sloučeny do jednoho dokumentu.

Základní data o dostupnosti a řešení incidentů dodá Objednatel Zhotoviteli během 3 (tří) pracovních dnů jako export z nástroje Service Desku MV.

2.2.13. Servisní řízení

Zhotovitel nejméně 60 (šedesát) dnů před uvedením AZYL III do provozu oznámí poskytovateli kontakty na Servisního manažera, tedy osobu odpovědnou za provoz a poskytování technické podpory IS AZYL III. V odpovědnosti servisního manažera bude:

- návrh procesů podpory (reviduje a schvaluje Objednatel), jejich zavedení u Zhotovitele,
- kontrolu dodržování nastavených procesů,
- průběžné hodnocení ukazatelů úrovně kvality služeb, při snížení náprava,
- účast v Change Advisory Board,
- účast na pravidelných provozních schůzkách,
- eskalační kontakt,
- reporting a akceptace služeb.

Projekt „Informační systém mezinárodní ochrany (IS AZYL III)“ (Registrační číslo: AMIF/11/01) je financován v rámci Národního programu Azylového, migračního a integračního fondu.

2.3. Definice rolí a odpovědností

Tabulka 3 – Definice rolí a odpovědností

Kapitola Přílohy č.2	Zhotovitel	Objednatel	Režim	Poznámka
2.2.1. Technická podpora HW a provozního prostředí				
Provoz, monitorování a zálohování infrastruktury a prostředí UPAAS		R	24x7	
Součinnost při úpravách prostředí AZYL III		R	24x7	
2.2.2. Technická podpora a maintenance SW				
Zajištění maintenance dodávaného SW, který tvoří AZYL III	R		8x5	Schvaluje CAB
Poskytování maintenance na operační systém		A, R	8x5	V případě MS OS
Analýzy dopadu aktualizací SW, který tvoří AZYL III vč. operačního systému	R		12x7 Zhotovitel, 24x7 Objednatel	
Instalace aktualizací SW, který tvoří AZYL III vč. operačního systému	R		8x5	Schvaluje CAB
Aktualizace a úpravy prostředí UPAAS a související infrastruktury	I	A, R	12x7 Zhotovitel, 24x7 Objednatel	
Analýza dopadu/Součinnost při aktualizacích a úpravách prostředí UPAAS a související infrastruktury	R	A	12x7 Zhotovitel, 24x7 Objednatel	
2.2.3. Řešení incidentů				
Řešení incidentů IS AZYL III	R	C	12x7 Zhotovitel, 24x7 Objednatel	
Součinnost při řešení incidentů související infrastruktury a prostředí UPAAS	R	A	12x7 Zhotovitel, 24x7 Objednatel	
Součinnost při řešení bezpečnostních incidentů	R	C	12x7 Zhotovitel, 24x7 Objednatel	
Poskytování platformy pro hlášení a evidenci incidentů - ServiceDesk MV		R	12x7 Zhotovitel, 24x7 Objednatel	DCeGOV - objednává u NAKITu
Řešení incidentů infrastruktury UPAAS a související infrastruktury	I	R	12x7 Zhotovitel, 24x7 Objednatel	Informace o incidentech, které mají vliv na AZYL III
Součinnost při řešení incidentů IS AZYL III	A	R	12x7 Zhotovitel, 24x7 Objednatel	
2.2.4. Řešení problémů				
Řešení problémů IS AZYL III	A, R	C	12x7 Zhotovitel, 24x7 Objednatel	
Řešení problémů UPAAS a související infrastruktury	C	A,R	12x7 Zhotovitel, 24x7 Objednatel	
2.2.5.1. Změny vyplývající z Řešení problémů				
Definice a návrh změny v AZYL III	R	C	12x7 Zhotovitel, 24x7 Objednatel	
Analýza dopadu změny	R	C	12x7 Zhotovitel, 24x7 Objednatel	
Schvalování realizace změny			8x5	Schvaluje CAB
Realizace změny	R		12x7 Zhotovitel, 24x7 Objednatel	
2.2.5.2. Úpravy funkcionalit v IS AZYL III dle potřeby Objednatele (Drobný rozvoj)				
Definice a návrh změny v AZYL III		A	8x5	
Analýza dopadu změny, nabídka na realizaci	R	C	8x5	
Schvalování realizace změny - dopad na systém			8x5	Schvaluje CAB
Schvalování realizace změny - finanční hledisko	C	A	8x5	
Realizace změny	R	I	8x5	
2.2.5.3. Změny realizované za účelem souladu s legislativou				
Definice a návrh změny v AZYL III	R	A, C	12x7 Zhotovitel, 24x7 Objednatel	
Schvalování realizace změny			8x5	Schvaluje CAB
Realizace změny	R	I	12x7 Zhotovitel, 24x7 Objednatel	
2.2.6. Údržba				
Údržba	R - za AZYL III	R - za UPAAS	12x7 Zhotovitel, 24x7 Objednatel	

2.2.7. Monitoring				
Provozování monitorovacího systému AZYL III	R - za AZYL III	R - za UPAAS	12x7 Zhotovitel, 24x7 Objednatel	
Úpravy nastavení monitorovacího systému AZYL III a dílčích testů pro monitorování funkčnosti aplikace a jejích klíčových komponent	R		12x7 Zhotovitel, 24x7 Objednatel	
Monitorování stavu aplikace AZYL III a jejích klíčových komponent, reakce na chybové stavy	R		12x7 Zhotovitel, 24x7 Objednatel	
Monitorování prostředí UPAAS, reakce na chybové stavy		R	12x7 Zhotovitel, 24x7 Objednatel	
Analýza událostí v monitorovacím systému	R - za AZYL III	R - za UPAAS	12x7 Zhotovitel, 24x7 Objednatel	
Poskytnutí součinnosti DCeGOV pro předávání a analýzu logů pro bezpečnostní dohled za IS AZYL III	R - za AZYL III	R - za UPAAS	12x7 Zhotovitel, 24x7 Objednatel	
Poskytnutí součinnosti při analýze SLA	R - za AZYL III	R - za UPAAS	12x7 Zhotovitel, 24x7 Objednatel	
2.2.8. Zálohování				
Provozování Systému zálohování a obnovy dat AZYL III	R - za AZYL III		12x7 Zhotovitel, 24x7 OPITK	
Nastavení zálohování	R - za AZYL III	R - za UPAAS	12x7 Zhotovitel, 24x7 Objednatel	
Realizace zálohovacích úloh, kontrola úspěšnosti záloh, řešení problémů	R - za AZYL III	R - za UPAAS	12x7 Zhotovitel, 24x7 Objednatel	
Realizace testů DR a testů funkčnosti obnovy záloh pro UPAAS		R	12x7 Zhotovitel, 24x7 Objednatel	
Pravidelné testování funkčnosti obnovy zálohovaných dat	R		12x7 Zhotovitel, 24x7 Objednatel	
Poskytnutí součinnosti Zhotoviteli AZYL III při obnově (včetně obnovy virtuálních serverů)		R	12x7 Zhotovitel, 24x7 Objednatel	
Poskytnutí součinnosti při řešení problémů realizace zálohování UPAAS	R		12x7 Zhotovitel, 24x7 Objednatel	
Realizace DR testů a funkčnosti obnovy pro AZYL III a součinnost pro DR testy prostředí UPAAS	R		12x7 Zhotovitel, 24x7 Objednatel	
2.2.9 Správa virtuálních serverů				
Správa virtuálních serverů na produkčním i testovacím prostředí	R		12x7 Zhotovitel	
Správa identit na virtuálních serverech a aplikačních částech	R		12x7 Zhotovitel	
Provozování prostředí UPAAS a související infrastruktury		R	24x7 Objednatel	
Součinnost při změnách konfigurace virtuálních serverů a poskytování informací o související infrastruktuře či prostředí UPAAS pro nastavení komunikačních toků AZYL III	C	R	24x7 Objednatel	
Součinnost při správě a provozu souvisejícího prostředí UPAAS	R	A	12x7 Zhotovitel, 24x7 Objednatel	
2.2.10. Součinnost na ověření DR				
Ustanovení DR procesu		A,R	12x7 Zhotovitel, 24x7 Objednatel	
Součinnost na ověření DR procesu	R - za AZYL III	R - za UPAAS	12x7 Zhotovitel, 24x7 Objednatel	
2.2.11. Součinnost při plánování dalšího rozvoje				
Součinnost při plánování dalšího rozvoje AZYL III	C	A	8x5	
2.2.12. Reporting a akceptace služeb				
Výkaz o dostupnosti AZYL III a plnění SLA	R		8x5	
Výkaz o řešení incidentů včetně dodržení Reakční doby, Doby vyřešení a příčiny incidentu	R		8x5	
Výkaz o řešení problémů	R		8x5	
Výkaz o čerpání Ad-hoc služeb	R		8x5	
Realizace schůzek s dodavatelem		R	8x5	
Akceptace/neakceptace výkazů		R	8x5	
Akceptace/neakceptace plnění SLA a případné řešení sankcí		R	8x5	
Finanční kontrola a plnění		R	8x5	

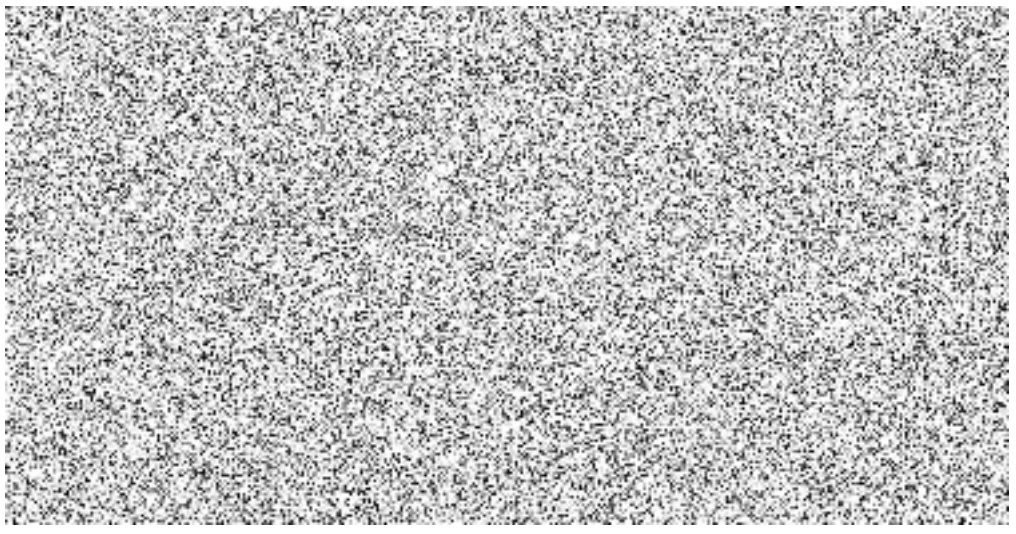
Vysvětlivky:

A - rozhoduje o provedení činnost

R - realizuje činnost

C - je konzultován, poskytuje součinnost

I - je informován



Projekt „Informační systém mezinárodní ochrany (IS AZYL III)“ (Registrační číslo: AMIF/11/01) je financován v rámci Národního programu Azylového, migračního a integračního fondu.