SPECIFIKACE SLUŽBY

podle ustanovení § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění (dále jen „ZZVZ"), k nadlimitní veřejné zakázce na služby

s názvem

„CLOUDINGOVÉ A HOSTINGOVÉ SLUŽBY PRO INFORMAČNÍ SYSTÉMY ISPOP A ENVIHELP - II"

Obsah:

1 ÚVOD 3
2 Popis řešení ISPOP a EnviHELP 3
3 Poskytování služeb provozu infrastruktury 4
3.1 Služba bezpečnost prostředí - KL001 7
3.2 Služba technického provozu a poskytování virtuální infrastruktury - KL002 13
3.3 Služba provozu Call Centra – KL003 23
3.4 Služba převzetí provozu – KL004 27
3.5 Služba předání provozu – KL005 29
3.6 Služba na vyžádání – KL006 31
4 Seznam zkratek 33
5 Technologická platforma ISPOP a EnviHELP 35

1 ÚVOD

Zadávací podmínky jsou uvedeny v souladu s § 36 odst. 3 ZZVZ v Zadávací dokumentaci identifikované Zadavatelem pod č.j.: CEN/50/1141/2018

Tato zadávací dokumentace vymezuje předmět veřejné zakázky a obsahuje specifikaci a minimální požadavky na cloudingové, hostingové a datové služeb pro zajištění provozu technologické platformy informačních systémů ISPOP (informační systém plnění ohlašovacích povinností) a EnviHELP (Environmentální helpdesk) .

ISPOP je významný informační systém dle vyhlášky č. 317/2014 Sb. NBÚ a MV a je zřízen zákonem č. 25/2008 Sb., o integrovaném registru znečišťování životního prostředí a integrovaném systému plnění ohlašovacích povinností v oblasti životního prostředí.

Dokument primárně popisuje služby technologické infrastruktury společné pro systémy ISPOP a EnviHELP.

2 Popis řešení ISPOP a EnviHELP

Architektura obou projektových úloh, ISPOP a EnviHELP, sdílí většinu dodávaných komponent a jen menší část je využívána pouze pro jednu projektovou úlohu. Typicky se jedná o aplikace, které realizují hlavní záměr dané projektové úlohy.

Jednotlivé aplikace jsou instalovány jak na fyzické servery, tak na servery virtuální. Fyzické servery jsou použity tam, kde je potřeba dosažení vysoké dostupnosti, velkého výkonu v IO operacích (databázové servery nebo veřejný portál) nebo výhodnějšího licencování. Virtuální servery pak poskytují základ pro všechny ostatní dodané aplikace, virtualizace pak v projektu zabezpečuje možnost upravovat výkon daných serverů dle aktuálních podmínek jejich vytížení, typicky v ohlašovacích špičkách apod.

Pro zajištění dostatečného aplikačního zázemí je na aktuální infrastruktuře použito virtuální prostředí nad VMware vSphere v edici Enterprise Plus a stejné zázemí se očekává zajistit i v rámci nové služby provozu infrastruktury.

3 Poskytování služeb provozu infrastruktury

Poskytovatel bude poskytovat Objednateli v souladu se Smlouvou služby (dále jen „**Služby**" nebo jednotlivě jen „**Služba**") blíže specifikované v katalogových listech (dále jen „**Katalogové listy**" nebo jednotlivě jen „**Katalogový list**" či „**KL**"):

- Služba bezpečnost prostředí – KL001
- Služba technického provozu a poskytování virtuální infrastruktury – KL002
- Služba provozu Call Centra – KL003
- Služba převzetí provozu – KL004
- Služba předání provozu – KL005
- Služba na vyžádání – KL006

Poskytovatel je povinen provést veškeré kroky a poskytnout veškeré plnění potřebné k dosažení stavu připravenosti pro zahájení řádného poskytování Služeb, jak jsou definovány v Katalogových listech (dále jen „**Připravenost**"). Připraveností se rozumí takový stav, za kterého je Poskytovatel schopen poskytovat řádně, včas a na dohodnuté úrovni Služby v souladu s KL005 a na něj navazujícími KL001-KL003 dle dojednaného harmonogramu přechodu.

Objednatel je oprávněn požadovat rozšíření nebo snížení množství odebírané služby, která povede k zvýšení či snížení poskytovaného výkonu virtuální infrastruktury (KL002). V případě zvýšení nebo snížení množství odebírané služby v průběhu doby trvání smlouvy dojde k nacenění změny odebíraných služeb na základě jednotkové ceny a to poměrným způsobem, který musí být prokazatelný. Změny služby související se škálováním výkonu jsou poskytovány bezplatně v rámci služby KL002.Poskytovatel v nabídce uvede, jaký dopad má zvýšení nebo snížení množství odebírané služby KL002 vliv na ostatní odebírané služby.

Poskytovatel je povinen poskytovat Služby a jakékoliv další plnění podle Smlouvy v souladu se všemi příslušnými právními národními předpisy, předpisy Evropské unie a aplikovat při plnění Smlouvy nejlepší osvědčené postupy, procesy a metody („best practices") příslušného odvětví. Stejně tak je Poskytovatel povinen poskytovat Služby v souladu se standardním prostředím Objednatele tak, aby byly vyloučeny možné negativní dopady do tohoto prostředí. Standardním prostředím se rozumí zejména využití stabilních, výrobci podporovaných komponent, jejich konfigurace v souladu s doporučeními výrobce a doporučeními provozovatelů aplikací (ve smluvním vztahu k Objednateli), a údržba firmware a software v aktuálním stavu, aby nedocházelo k bezpečnostním rizikům.

Poskytovatel je povinen poskytovat služby, které jsou předmětem Smlouvy, pouze prostřednictvím zaměstnanců a jiných osob odborně způsobilých k poskytování plnění (tzv. členů realizačního týmu), kterými v rámci zadávacího řízení prokazoval kvalifikaci. Každá změna ve složení realizačního týmu

musí být předem písemně schválena Objednatelem a složení realizačního týmu musí respektovat kvalifikační požadavky na realizační tým obsažené v zadávací dokumentaci.

Objednatel je oprávněn požadovat Služby obsažené v KL006 formou písemné objednávky, a to v přiměřeném rozsahu dle aktuálních podmínek vyžadovaných legislativou a stavem na infrastruktuře provozovaných aplikací za využití cen za člověkoden, které odpovídají cenám služeb v místě a čase obvyklým, maximálně však do výše ceny stanovené smlouvou. Služby obsažené v KL006 se mohou týkat pouze Služeb obsažených v KL001 – KL005 a musí projít finanční kontrolou na straně Objednatele.

Pravidla při aplikaci hodnocení SLA

1. Pokud se na tentýž výpadek vztahuje více hodnocení SLA (např. výpadek služby je zároveň výpadkem bezpečnostním), uplatní se sankce za výpadek jen jednou, a to v té službě, která má nejvyšší úroveň postihu.

2. Postihy za jednotlivá nedodržení úrovně SLA se v rámci fakturačního období sčítají. Pokud je však příčinou výpadku Datové centrum, uplatní se přednostně sankce za nesplnění provozu datového centra a k sankcím za navazující služby se již nepřihlíží.

3. Postih za nedodržení úrovně SLA se uplatní v tom měsíci, kdy se výpadek služby zjistil (nastal). Nebyla-li uplatněna sankce za výpadek v tomto období, přesouvá se její uplatnění do nejbližšího fakturačního období.

4. Za dostupnost služby, se považuje doba a kvalita poskytovaného plnění v rozsahu stanoveném katalogovými listy. Je-li služba vybavena možností záložního zpracování (např. active-pasive), pak provoz na záložním prostředí se za výpadek nepovažuje.

5. Maximální sleva z plnění je 100% z ceny katalogového listu poskytované služby za měsíc (dané období).

6. Sankce ani jiné postihy nemohou být uplatněny za neplnění SLA, pokud se jednoznačně prokáže, že neplnění SLA nebylo způsobeno Poskytovatelem a Poskytovatel nemohl toto neplnění SLA nijak ovlivnit.

3.1 Služba bezpečnost prostředí - KL001

Kód služby	**KL001**
Název služby	**Služba bezpečnost prostředí**
Cíl služby	Cílem služby je zajištění zvýšené bezpečnosti provozu poskytovaných infrastrukturních služeb.
Popis služby	**Obecné požadavky** Řízení bezpečnosti zahrnuje tyto ICT oblasti: • datové centrum (DC) • komunikační infrastrukturu • serverovou a datovou infrastrukturu • virtuální infrastrukturu – tím je myšleno nejméně datové centrum (fyzicky), komunikační infrastruktura (sítě vč. aktivních prvků), servery (fyzické vč. komponent, racky, chassis, switche, virtualizace a operační systémy, systémové služby (zejména zálohování, updaty) • Systémové služby – zajišťují spolupráci mezi jednotlivými systémy, zajišťují bezpečný přístup ke službám a aplikacím apod. Poskytovatel musí dokumentovat bezpečnostní politiku v souvislosti s poskytovaným plněním, operační procedury a provozní postupy a seznamovat s dokumentací všechny dotčené strany s oprávněným přístupem k nim. Poskytovatel zajistí služby v souladu s požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti v platném znění a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění, a jeho prováděcími předpisy v návaznosti na změny prováděné v ostatních katalogových listech. Tento soulad bude dokumentován. Poskytovatel se musí též řídit pravidly příslušné části bezpečnostní dokumentace Zadavatele Poskytovatel provádí opatření v následujících oblastech: • Organizační a personální bezpečnost ◦ Poskytovatel musí splňovat podmínku své bezúhonnosti i bezúhonnosti osob zajišťujících plnění Smlouvy po celou dobu její platnosti. ◦ Poskytovatel nepřipustí poskytování služeb pomocí technických prostředků mimo vlastní ICT infrastrukturu (privátní cloud). V rámci privátního cloudu mohou být prostředky mezi službami Objednatele sdíleny či dedikovány. ◦ Poskytovatel zajistí po celou dobu poskytování služeb efektivní provoz svého systému řízení bezpečnosti informací podle obecně uznávané metodiky ISO/IEC 27 001 pro poskytované služby. ◦ Poskytovatel zajistí realizaci změn v přístupových právech fyzických (do objektů) i logických (k systémovým komponentám) v důsledku změn v zařazení pracovníků, kteří měli/mají přístup. ◦ Poskytovatel zajistí, že každý, kdo vstupuje do prostor DC, má vyřízeny patřičné náležitosti nutné pro vstup, je seznámen s provozním řádem DC a poučen o svých povinnostech. ◦ Seznamování osob s provozním řádem DC a poučení osob s právem přístupu do DC provádí Poskytovatel opakovaně a vede o tom evidenci.

- Poskytovatel vede evidenci vstupů osob do DC.
- Poskytovatel poskytne evidenci vstupů, seznamování osob s provozním řádem a s poučením na vyžádání Objednateli (formou nahlédnutí na místě).
- Poskytovatel po dobu přítomnosti osob třetích stran v DC zajistí jejich trvalé doprovázení pracovníky Poskytovatele, kteří byli seznámeni s provozním řádem DC a poučeni o svých povinnostech.
- Poskytovatel poskytne spojení na kontaktní fyzické osoby pro podporu řešení problémů s provozem informačních systémů (IS) Objednatele. Poskytovatel je povinen spolupracovat při řešení problémů bezpečnostních) s Poskytovateli aplikací a ostatních programových komponent (třetími stranami).
- Poskytovatel zajistí, aby v případě náhrady technického zařízení jiným zařízením (např. diskových polí z důvodu zvýšení rychlosti či kapacity) byla veškerá data na nahrazovaném zařízení bezpečně zničena (pochopitelně včetně těch, která jsou uložena permanentně, tj. i po odpojení od zdroje napájení). Za zničení dat je považován nejméně přepis kompletního obsahu datových médií hodnotou „0" v každém byte kapacity, případně standardizované postupy používané v ICT, pokud to daná součást vyžaduje a je to technicky možné. Do doby zničení dat nesmí být zařízení využito k jiným účelům mimo prostředí infrastruktury Objednatele.
- Poskytovatel musí udržovat aktuální vlastní bezpečnostní směrnice a na vyžádání je Objednateli předložit minimálně k nahlédnutí.
- Poskytovatel musí mít nastaveny efektivní a evidované procesy Change a Incident Managementu a na vyžádání je předložit oprávněným pracovníkům Zadavatele minimálně k nahlédnutí.
- Poskytovatel po celou dobu trvání Smlouvy musí v rámci Change a Incident Managementu vést evidenci veškerých změn týkajících se infrastruktury užívané pro Objednatele a tyto změny na vyžádání Objednatele předložit. Dále pak je Poskytovatel povinen tyto změny předložit Zadavateli vždy k 31. prosinci, po dobu platnosti Smlouvy, a rovněž ke dni ukončení jeho aktivit plynoucích ze Smlouvy se Objednatelem.
- Poskytovatel zajistí ochranu proti násilnému fyzickému vniknutí do prostor DC z prostor mimo DC.
- Poskytovatel zajistí 24 hodinovou ostrahu s připojením systému EZS k pultu centralizované ochrany PČR, bezpečnostní agentury či ekvivalentní formu dohledu.
- Poskytovatel zajistí CCTV způsobem, že monitoruje vstup oprávněných osob do datového sálu; Poskytovatel zajistí, aby tento monitoring byl v souladu s platnou legislativou.
- Poskytovatel zajistí systém perimetrické ochrany datového sálu (tzn. Poskytovatel preventivně zjišťuje bezpečnostní incidenty a efektivně je řeší ještě mimo vlastní sál DC - např. zajištěním ochrany celého objektu, kde je datový sál provozován).
- Poskytovatel zajistí ochranu proti požáru, formou napojení na elektronický protipožární systém (EPS) s neustálým dohledem a hasicími plyny nepoškozujícími elektroniku (systém minimálně s čidly kouře, teploty, vlhkosti) - stabilní hasicí zařízení (SHS).
- Poskytovatel zajistí propojení systému EPS s pultem centralizované ochrany Hasičského záchranného systému (HZS) nebo bezpečnostní agentury.
- Poskytovatel zajistí monitoring teploty sálu a jednotlivých racků se vzdáleným přístupem k těmto informacím pro oprávněné osoby.
- Poskytovatel zajistí ochranu proti vytopení DC zevnitř, formou napojení na EZS s neustálým dohledem.
- Poskytovatel zajistí detekci zaplavení sálu.
- Poskytovatel zajistí režim ostrahy a připojení výše uvedených systémů

v režimu 24x7.

- Poskytovatel zajistí způsob ostrahy znemožňující fyzický přístup nepovolaným osobám.
- Poskytovatel zajistí řízený přístup k systémovým komponentám a to minimálně s ověřením ostrahou a kartou.
- Poskytovatel zajistí logování událostí ACS a uchování logů včetně logů EZS, EPS a záznamů CCTV. Logy EZS a EPS uchovává minimálně po dobu 6 měsíců, záznamy z CCTV uchovává po dobu nejméně 1 měsíce.
- Poskytovatel umožní Objednateli a jím určeným osobám přístup k záznamům CCTV a logům EZS a EPS minimálně k nahlédnutí.
- Poskytovatel zajistí nemožnost změny pořízených záznamů a logů.
- Poskytovatel zajistí provozní podmínky zařízení pro poskytované služby dle doporučení výrobce.
- Veškeré výše uvedené služby budou dokumentovány.

- **Fyzickou bezpečnost**

  Poskytovatel DC zajistí splnění požadavků kategorie min. TIER III DC. Lze využít certifikát TIER III DESIGN dle UPTIME institute nebo předložit jiné důvěryhodné dokumenty, které dokládají splnění požadavků v rozsahu certifikace TIER III DESIGN dle UPTIME institute.

  Jsou požadovány vlastnosti zejména:

  - Zajistit redundanci všech klíčových prvků:
    - o Zajistit redundanci napájecích okruhů, tj. napájení nejméně ze dvou rozdílných směrů.
    - o Zajistit redundanci síťových přípojek tj. připojení k nadřazené síťové infrastruktuře nejméně ze dvou rozdílných směrů s tím, že trasy vedení síťového spojení nejsou totožné s trasami vedení napájení.
    - o Zajistit redundanci aktivních síťových prvků (přepínačů a směrovačů) přímo v DC.
    - o Zajistit redundanci ventilace.
    - o Zajistit redundanci chlazení.
    - o Zajistit redundanci zdrojů (napájení) serverů: fyzické servery obsahují nejméně dva zdroje s tím, že zdroje jsou napojeny každý na jiný okruh napájení.
  - Zajistit náhradní napájení pro provoz technologií Objednatele a souvisejících technologií DC nejméně na 24 hod.
  - Zajistit pravidelné kontroly funkce všech záložních napájecích zdrojů nejméně jednou ročně a vede o tom zápisy, které je schopen na vyžádání předložit.
  - Zajistit pravidelnou údržbu hardware a vede o tom zápisy, které je schopen na vyžádání předložit.
  - Zajistit lokální zdroj přesného času, který využijí všechny instalované prvky v DC. Zajistí synchronizaci času lokálního zdroje času nejméně jednou denně.
  - Zajistit auditovatelný dohled nad Objednatelem požadovanými systémy minimálně po dobu Objednatelem požadovanou a na vyžádání o něm poskytne informace Objednateli.
  - Instalované technologie budou monitorovány Poskytovatelem. Poskytovatel infrastruktury zajistí bezodkladné informování Objednatele a jím určených osob o závadách a zhoršení provozních parametrů systémových komponent, které mají nebo mohou mít vliv na informační aktiva Objednatele dle parametrů definovaných ve Smlouvě.
  - Zajistit striktní oddělení jednotlivých OS způsobem využívajícím virtualizační prostředí.
  - Umožnit umístění kompletního prostředí včetně operačních systémů a aplikací do virtuálních strojů bez závislosti na provozovaném hardware kromě výjimek

jednoznačně vyplývajících z omezení virtuálních strojů stanoveného jejich výrobcem nebo objednavatelem.

- Umožnit využití dedikovaného hardware pro instalaci software (operační systém, databáze.)
- Bezpečnostní dohled a správa bude provozována z jednoho místa, které má záložní řešení.
- Zajistit pravidelné provádění skenů externí a interní zranitelnosti nejméně jednou ročně a při významné změně systémových komponent. Na vyžádání poskytne informaci o provedených testech.
- Umožnit po vzájemné dohodě provádění skenů externí a interní zranitelnosti na požadavek Objednatele nebo jím určené osoby. Rozsah součinnosti Poskytovatele nepřekročí 3 člověkodny za rok.
- Používat techniky detekce a prevence narušení v souladu s oborovými standardy, udržovat je aktualizované.
- Zajistit mechanismus detekce změn konfigurace systémových komponent a řízenou reakci na tyto změny, která zahrnuje informování Objednatele.
- Zajistit trvalý vzdálený přístup Objednatele k systémovým logům pro jednotlivé komponenty infrastruktury souvisejících s poskytovaným plněním a zamezit neoprávněnému přístupu třetích stran k záznamům týkajících se systémů Objednatele.
- Zajistit nástroj pro zajišťování úrovně dostupnosti služeb požadované dle infrastrukturních, případně aplikačních SLA a správu tohoto nástroje.
- Sledovat veřejně známé zranitelnosti a reaguje na ně ve vztahu s poskytovanými službami. Zejména dbát rychlé adekvátní reakce na zjištění kritické zranitelnosti.

Pro zajištění monitoringu a správy provozní bezpečnosti není nutno využívat jen dedikované prostředky pro Objednatele, ale je nezbytné zajistit, aby se chybnou architekturou, konfigurací či jinými možnostmi nesnižovala bezpečnost provozu infrastruktury Objednatele (např. Neoprávněným výdejem dat třetím stranám o provozu Objednatele, zvýšení zranitelnosti prostředí Objednatele atp.).

- Ochrana dat
  - Poskytovatel umožní využít pro stávající systémy definované touto Smlouvou nástroj pro ověřování identity uživatelů v souladu se standardy LDAP a Active Directory. Umožní Objednateli a třetím stranám (Poskytovatelům aplikací) uživatelský přístup za účelem konfigurace ověřování a provádění ověřování.
  - Poskytovatel umožní využít pro stávající systémy definované touto Smlouvou nástroj pro řízení přístupových oprávnění. Umožní Objednateli a třetím stranám (Poskytovatelům aplikací) uživatelský přístup za účelem konfigurace ověřování a provádění ověřování.
  - Poskytovatel zajistí nástroj pro ochranu před škodlivým kódem na úrovni perimetru DC, jeho pravidelnou aktualizaci a automatizovaný sběr údajů.
  - Poskytovatel zajistí nástroj pro zaznamenávání činností informační infrastruktury a informačních systémů, jejich uživatelů a administrátorů. Zajistí sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci systémové komponenty, která činnost zaznamenala, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti a ochranu získaných informací před neoprávněným čtením nebo změnou.
  - Poskytovatel zajistí nástroj pro zaznamenávání činností komponent vztahujících se k předmětu plnění zaznamenaných do systémových logů způsobem, který zaznamenává nejméně:

- o přihlášení a odhlášení uživatelů a administrátorů,
- o činnosti provedené administrátory,
- o činnosti vedoucí ke změně přístupových oprávnění,
- o neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
- o zahájení a ukončení činností systémů,
- o automatická varovná nebo chybová hlášení systémů,
- o přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností,
- o použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

- Poskytovatel zajistí nástroj pro detekci kybernetických bezpečnostních událostí (IDS/IPS) na úrovni perimetru DC,

- Na žádost Objednatele Poskytovatel poskytne podklady (logy) a spolupráci pro analýzu provozu/incidentů automatizovanými nástroji.
  - Poskytovatel zajistí administrátorský deník vedený v zabezpečené elektronické podobě. Zajistí povinnost administrátorů pořizovat záznamy do administrátorského deníku. Pravidelně kontroluje soulad obsahu administrátorského deníku s údaji nástroje pro zaznamenávání činností informační infrastruktury a informačních systémů, jejich uživatelů a administrátorů; v případě nesouladu informuje Objednatele a jím vyznačené subjekty.
  - Poskytovatel zajistí ochranu záznamů (logů) proti změně a neautorizovanému přístupu.
  - Poskytovatel po vzájemné dohodě umožní externím subjektům provedení auditu informační bezpečnosti. Rozsah součinnosti Poskytovatele nepřekročí 3 člověkodny za rok.
  - Poskytovatel zajistí zálohování dat způsobem, který zajistí bezpečné uchování záloh (proti fyzické destrukci i proti neoprávněnému přístupu).
  - Poskytovatel zajistí plány obnovy po havárii technického prvku do času stanoveného Objednatelem.
  - Poskytovatel umožní šifrování logických disků.
  - Poskytovatel umožní šifrování databází.
  - Poskytovatel zajistí dodržení standardů bezpečnosti přístupu k šifrovacím klíčům, za které odpovídá, a jejich pravidelnou obměnu.
  - Poskytovatel zajistí plány obnovy systémových komponent a jejich přezkoušení nejméně 1x za rok.
  - Poskytovatel zajistí sledování dostupnosti záplat instalovaných produktů a jejich řízenou instalaci.
  - Poskytovatel umožní řízený upgrade SW a zařízení na vyšší verzi, na základě dohody s Poskytovateli aplikací a Objednatelem.

- Síťová bezpečnost
  - Poskytovatel zajistí, že prostředí aplikací Objednatele a aplikací jiných správců je odděleno firewallem případně jinými prostředky.
  - Poskytovatel umožní, aby prostředí jednotlivých aplikací Objednatele bylo odděleno firewallem případně jinými prostředky.
  - Poskytovatel umožní instalaci a správu firewallů (případně jiných obdobně účinných prostředků) mezi front-end (prezentační vrstvu) a back-end informačních systémů.

  - Poskytovatel zajistí firewall (případně jiný obdobně účinný prostředek) na perimetru DC.

	• Poskytovatel zajistí nástroj pro ochranu proti DOS a DDoS útokům na perimetru DC. • Poskytovatel zajistí vzdálený administrátorský přístup způsobem, který zajistí logování činností administrátorů. • Poskytovatel zajistí pravidelnou změnu hesel / přístupových klíčů / certifikátů a dalších využívaných autentizačních a autorizačních objektů ke konfiguraci systémových komponent. • Poskytovatel zajistí splnění požadavků na hesla v kompetenci Poskytovatele v souladu s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění, a jeho prováděcími předpisy (např. vyhláška č. 316/2014 Sb.). • Poskytovatel zajistí konfigurační standardy routerů a firewallů (případně jiných obdobně účinných prostředků). • Poskytovatel zajistí zálohování konfigurací systémových komponent při nasazování změn. • Poskytovatel zajistí implementaci anti-spoofingových opatření na perimetru DC a kontrolu jejich účinnosti nejméně 1x ročně. O zjištěných nedostatcích informuje Objednatele. • Poskytovatel zajistí aktualizaci Dokumentace skutečného provedení nejméně 1x ročně. • Poskytovatel umožní VPN přístup na úrovni operačního systému. • Poskytovatel zajistí použití šifrovacích klíčů infrastruktury Poskytovatele v souladu s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění, a jeho prováděcími předpisy (např. vyhláška č. 316/2014 Sb.). • Poskytovatel zajistí bezpečnost přístupu k šifrovacím klíčům infrastruktury Poskytovatele. • Poskytovatel umožní dvoufaktorové ověření identity pro vzdálený přístup. • Poskytovatel umožní SSL (Secure Sockets Layer) terminaci. • Poskytovatel zajistí provoz protokolů IPv4 a IPv6 ve své síti a zajistí pro ně stejnou konektivitu do externích sítí se stejnou úroveň bezpečnosti. • Poskytovatel zajistí monitoring stavu konektivity DC do/z internetu z hlediska dostupnosti a vytížení. Monitoring aktivně upozorňuje na vybočení ze stanovených limitů. • Poskytovatel umožní po vzájemné dohodě sběr a ukládání záznamů o síťovém provozu (záznamy typu NetFlow). Umožní Objednateli přístup k nemodifikovaným záznamům o provozu jeho informačních systémů. Poskytovatel se zavazuje dodržovat principy ITIL a je povinen zajistit účast expertů na jednání, pokud si je Objednatel vyžádá.
Režim služby	Režim 7 x 24 Při výpadku služby je Poskytovatel povinen bezodkladně informovat Objednatele o výpadku, o obnovení služby; dále je Poskytovatel povinen: V pracovní dny v čase od 8:00 do 18:00 do 60 minut od výpadku písemně informovat Objednatele o stavu a zjištěných příčinách/důsledcích; do 24 hodin od obnovení služby podat komplexní písemnou zprávu o příčinách a důsledcích výpadku i o nápravných opatřeních. V ostatním čase pak do 9:00 hodin následujícího pracovního dne po výpadku písemně informovat Objednatele o stavu a zjištěných příčinách/důsledcích a do 24 hodin od této informace podat komplexní písemnou zprávu o příčinách a důsledcích výpadku i o nápravných opatřeních. Po dobu 24 hodin denně disponovat telefonním číslem („hotline"), kde je možno

	oznámit případný problém, resp. zjistit stav průběhu nápravy.

3.2 Služba technického provozu a poskytování virtuální infrastruktury - KL002

Kód služby	KL002
Název služby	**Služba technického provozu a poskytování virtuální infrastruktury**
Cíl služby	Cílem služby je poskytování virtuální a fyzické infrastruktury a souvisejících služeb pro provoz aplikace Objednatele v datových centrech Poskytovatele.
Popis služby	**Společné služby** **Požadavky na bezpečnost:** • Služba bude poskytována v souladu s KL001 **Požadavky na datová centra:** Poskytovatel má k dispozici dvě produkční datová centra splňující bezpečnostní požadavky uvedené v katalogovém listu KL001 a dále pak další datové centrum pro umístění arbitrážního systému (kvůli clusterům). Produkční datová centra (DC) jsou propojena dostatečně výkonným a bezpečným datovým spojením umožňující geografické rozložení dat a dále pak bezpečně propojena s datovým centrem pro umístění arbitrážního systému (komunikujícím s oběma DC). Produkční datová centra nesmí být umístěna ve stejném areálu či bloku budov; jejich vzdálenost musí být řešena tak, aby jejich propojení svou latencí a prostupností neomezovalo možnosti rozloženého zpracování mezi centry v reálném čase na straně jedné (tj. doporučené vzdálenosti kabelového vedení do 40 km) a zároveň dávalo jistotu provozu i při významném poškození (zničení) jednoho z center (tj. vzdálenost alespoň 5 km vzdušnou čarou). Produkční datová centra musí být k Internetu připojena v režimu geografické redundance, tedy v případě výpadku jednoho z datových center je Internetový provoz automaticky přesměrován do druhého datového centra Poskytovatele. Datová centra (produkční) musí splňovat: • Dostupnost DC a jeho infrastruktury minimálně 99,99%. • Redundance N+1 všech kritických systémů zajišťující servisovatelnost za provozu. • Konfigurace datových sálů v členění studená/teplá ulička nebo obdobný systém. • Zajištění standardních provozních teplot vhodných pro provoz informačních technologií. • Přesné jednotky klimatizace s nutností vzdálené správy. Telekomunikační infrastruktura odpovídající úrovni požadovaných služeb. Podlaha antistatická s opatřeními snižujícími prašnost. Nosnost podlah DC umožňující instalovat standardní 19" racky. Monitoring a dohled celé infrastruktury 24 x 7 lokality DC.

- **Prostředí (napájení, klimatizace)**
  - El. energie.
  - HVAC (22±3°C, 40%-60%).
  - Detekce kouře a hašení.
  - Možnost využít samostatných prostor pro práci pracovníků Objednatele a Poskytovatelů přímo v lokalitě datového centra.
- **Konektivita**
- Konektivita do internetu.
- Poskytovatel umožní realizovat požadavky na připojení jednotlivých pracovišť subjektů státní správy, samosprávy a jejich dalších datových a technologických center
- Infrastruktura je připravena na přechod na protokol IPv6.
- Poskytovatel zajistí datové linky do DC s výkonem min. 2x1 Gbps a možností postupného navyšování na řádově vyšší kapacitu podle aktuálních potřeb aplikací provozovaných na infrastruktuře.
- Datové linky musejí mít dostatečný přenosový výkon, a to i v případě jejich sdílení nižší přenosové vrstvy.
- Virtuální a fyzické servery v datových centrech Poskytovatele musí mít možnost spolu komunikovat v rámci jedné sítě (L2 propojení).
- Zajištění přístupů dle znění zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů.
- Integrace VPN přístupů za využití VPN koncentrátoru.
- Služba firewallů.
- Služba LAN přepínačů

Tato služba nebude zahrnovat poskytování a údržbu lokálních síťových infrastruktur u Objednatele a přidružených organizací.

- **Zajištění přístupů k datovým sítím**
- Poskytovatel zajistí přístup pro správu serverů, resp. dalších jím provozovaných komponent buď přímým přístupem, anebo prostřednictvím veřejné VIP (virtuální IP adresa), nebo přes VPN přístup, kdy VPN přístup je považován za optimální způsob pro přístup ke správě.
- Poskytovatel zajistí možnost vytváření privátních VLAN (Virtual Local Area Network).

- **Služba monitoringu**

Poskytovatel poskytuje službu monitoringu jednotlivých prvků infrastruktury, za které odpovídá v následujícím rozsahu:

- Provoz systému pro monitoring provozu HW, virtualizační platformy,

provozovaného ostatního základního SW, servicedeskového systému.
- V rámci této služby je úkolem poskytovat dohled nad infrastrukturou spočívající ve zjišťování funkčnosti jejich klíčových parametrů. V případě porušení nastavených prahových hodnot budou odesílány informace na odpovědné řešitelské skupiny Poskytovatele.
- Součinnost se třetími stranami (řešení incidentů, předání informací o problémech, požadavků na změny a configuration management v rámci služeb ServiceDesku).
- Tvorba a údržba provozní dokumentace.

- **Služba Syslog**
  Cílem služby je poskytnout prostředí pro logování událostí infrastruktury s možností
  jejich zpětné analýzy v souladu s požadavky v KL001.

- **Procesní provázanost služeb**
  - Poskytovatel umožní provedení změn vyplývajících z legislativních požadavků na provoz IS státní správy resp. ISO/IEC 20000 a ISO 27000

- **Požadovaná součinnost Poskytovatele**
  - Kontinuální tvorba a údržba dokumentace prostředí.
  - Správa virtualizačního SW.
  - Návrh, posuzování, realizace a dokumentace konfiguračních změn dle požadavků Objednatele v součinnosti s 3. stranami.
  - Změny konfigurací v rozsahu běžného provozu.
  - Patchování a přechody na nové verze (nasazování nových verzí aplikací vyžadující test na speciálně vytvořeném prostředí však spadají do KL006).
  - Komunikace a součinnost s 3. stranami v případě problémů či specifikace požadavků a návrhu řešení na základě podnětu Objednatele.

Požadavky na zálohování a obnovy **(služby Managed Backup):**
- Služba zahrnuje provoz, správu a monitoring zálohovacího HW a SW Poskytovatele, analýzu dat, konzultace při definici plánu zálohování.
- Návrh zálohovací politiky s ohledem na potřeby zadavatele
- Zálohování dle Objednatelem odsouhlasené zálohovací politiky.
- Obnova v případě havárie.
- Testování obnovy v rámci testování havarijních plánů v souladu s KL001.
- Součinnost se třetími stranami (řešení incidentů, požadavků na změny a configuration management v rámci služeb ServiceDesku).
- tvorba a údržba provozní dokumentace.
- souhrnná rychlost zálohování musí být min. 400 MB/sec.
- Služby zálohování musí efektivně využívat kombinaci řešení VTL a TL.
- Součástí služby musí být všechny potřebné licence zálohovacího SW, včetně licencí pro On-line zálohování RDBMS Oracle, AD.
- Vytvoření speciální kopie dat dle požadavků Objednatele.
- Datové kapacity jsou zálohovány s dostupností min. 1 měsíce v plném objemu, logy se zálohují podle zálohovacích plánů minimálně po dobu 3 měsíců pro Syslog, DB.
- K dispozici jsou kapacity pro zálohování v objemu, který zajišťuje logování průběžných změn aplikací, denní zálohy udržované zpětně po dobu

1 měsíce a až 3 dlouhodobé zálohy dle potřeb a určení Objednatelem pro každou aplikaci.

- Zálohy se v případě provozu aplikace jen v jednom datovém centru vždy ukládají v geograficky vzdáleném datovém centru s úrovní Tier 3. Předpokládaný měsíční objem záloh je 20TB.

Retenční doba zálohy 4 týdny

Předmětem je zajištění obnovy systému 4 týdny zpětně. Zálohovací politiku navrhne dodavatel s tím, že musí být dodrženy následující požadavky:

Záloha celého systému ISPOP 1 denně s následujícími výjimkami:

Záloha přijatých dokumentů 1 za hodinu

Záloha metadat přijatých dokumentů 1 za hodinu

Záloha databází 1 denně, záloha databázových logů 1 za 2 hodiny

Záloha celého systému EnviHELP 1 denně.

Dodavatel musí být schopen ze záloh provést obnovu celého systému.

Služba poskytování virtuální infrastruktury X86/X64

Služby zahrnuje:

- Alokaci a správu virtuálního výkonu.
- Virtualizaci na platformě VMWare v edici VMware vSphere Enterprise Plus a verzi 6.0 a novější.
- Servery budou umístěny v DC1, DC2 splňující parametry uvedené výše a v KL001.
- Požadovaná platforma - Intel x86/x64 kompatibilní.
- Vyžadované prostředí pro provoz aplikací: Windows 2008 R2 a novější, CentOS 6 a novější, OS RedHat Linux 6 a novější, SLES 11.4 a novější.
- Poskytovatel umožní v dohodnutých případech administraci OS Objednatelem.
- Přípustný agregační poměr na virtualizační platformě je pro CPU 3:1 (tedy 3vCPU na jedno fyzické jádro) a pro RAM 1:1 (bez agregace).
- Řešení musí podporovat MSCS clustery (OS Windows 2008 R2 a novější) a RedHat Linux clustery (OS RedHat Linux 6 a novější).
- Podpora a administrace až do úrovně provozu engine databáze, není-li dohodnuto jinak.

Služba virtuálních serverů

Příklad minimální konfigurace:

ProLiant BL460c Gen8, nebo ekvivalent a vyšší

CPU 2x Intel(R) Xeon(R) CPU E5-2665 0 @ 2.40GHz (8 Cores)

RAM 256 GB

NET 6x 1Gb LOM

HBA 2x FCoE FlexHBA 10Gb

HDD No internal storage

HW Management ILO

Minimální parametry virtuálních serverů jsou uvedeny v kapitole 5

Pro servery uvedené v tabulce výše tohoto katalogového listu má Objednatel nárok na až 10 % navýšení počtu/výkonu virtuálních serverů za každý rok Smlouvy bez navýšení ceny, dle požadavků Objednatele.

Služba fyzických serverů

Příklad minimální konfigurace **2ks:**

ProLiant BL460c Gen8, nebo ekvivalent a vyšší

CPU 1x Intel(R) Xeon(R) CPU E5-2609 @ 2.40GHz (4 Cores)

RAM 96 GB

NET 6x 1Gb LOM

HBA 2x FCoE FlexHBA 10Gb

HDD No internal storage

HW Management ILO

Minimální parametry fyzických serverů jsou uvedeny v kapitole 5

Lokalita	Název serveru	Paměť [GB]	CPU [počet jader]	Poznámka
DC1	DB1	96	4	databázový server – cluster node #1

Lokalita	Název serveru	Paměť [GB]	CPU [počet jader]	Poznámka
DC2	DB2	96	4	databázový server – cluster node #2

Služba Licencování

Pro podporu jednotlivých agend je využívána služba licencování, tj. poskytnutí licencí formou služby.

- VMware vSphere Enterprise Plus ve verzi 6.0 a novější pro zajištění virtualizace všech serverů Objednatele
- 4x OS – Red Hat Enterprise Linux Server subscription Standard
- Adobe LifeCycle Enterprice Suite pro provoz serverů ADOBE-1 a ADOBE-2
- Oracle Database Standard Edition 2

Poskytovatel zajistí průběžnou podporu všech licencí, včetně možnosti upgrade na vyšší verze.

Služba provozu aplikace

Prostředí a služby:

- Fyzický databázový geocluster (platforma x86)
- Virtuální georedundandní prostředí pro aplikace (platforma x86)
- Synchronní replikace dat mezi DC (RPO = 0)
- Podpora OS a engine DB

	• Zálohování • Dokumentace infrastrukturního prostředí • Konektivita • Dohledy • Vystavení aplikace do produkce Poskytovatel se zavazuje dodržovat principy ITIL a je povinen zajistit účast expertů na jednání s Poskytovatelem podpory a rozvoje jednotlivých aplikací alespoň jedenkrát za týden pro každou z aplikací (tato četnost jednání a účast expertů se nevztahuje k případům řešení incidentu, kde je potřeba se účastnit dle reálné potřeby rychlého řešení), pokud si je Objednatel vyžádá. Objednatel může čerpat nevyužité kapacitní a výkonové meziroční nárůsty stanovené touto Smlouvou též jejich adekvátní transformací na jiné služby popisované v katalogových listech této Smlouvy. Takové změny musí být odsouhlaseny oběma smluvními stranami. Poskytovatel se zavazuje změnit kapacitu odebíraných služeb na základě požadavků Objednatele. Průměrná roční kapacita poskytovaných služeb odpovídá požadavkům v kapitole a jejich cena se tak nemění.

SLA parametry dostupnosti služby			
Služba	Dostupnost služby měsíční (v %)	Rozsah zaručeného provozu služby	Max.doba jednoho výpadku služby (v minutách)
Dostupnost virtuální a fyzické infrastruktury včetně služeb dohledu	99,00	24 x 7	120
Datového centra včetně konektivity	99,99	24 x 7	30
Služby potřebné k provozování OS, DB, úložiště dat, zálohování a komunikační infrastruktury aplikací	98,00	24 x 7	120

SLA parametry řešení incidentů

Při výpadku služby je Poskytovatel povinen bezodkladně informovat Objednatele o výpadku, o obnovení služby; dále je Poskytovatel povinen:

V pracovní dny v čase od 8:00 do 18:00 do 60 minut od výpadku písemně informovat Objednatele o stavu a zjištěných příčinách/důsledcích; do 24 hodin od obnovení služby podat komplexní písemnou zprávu o příčinách a důsledcích výpadku i o nápravných opatřeních.

- V ostatním čase pak do 9:00 hodin následujícího pracovního dne po výpadku písemně informovat Objednatele o stavu a zjištěných příčinách/důsledcích a do 24 hodin od této informace podat komplexní písemnou zprávu o příčinách a důsledcích výpadku i o nápravných opatřeních.

Parametr	Popis	Priorita	Doba	Plnění (v%)
Doba vyřešení	Dobou vyřešení se myslí čas, který uplyne od akceptace Incidentu / Servisního požadavku do doby vyřešení Incidentu / Servisního požadavku. Do Doby vyřešení není započítáván čas čekání na součinnost Objednatele nebo Poskytovatele Objednatele.	Priorita 1	do 2 pracovních hodin	85,00
		Priorita 2	do 5 pracovních hodin	85,00
		Priorita 3	do 1 pracovního dne	85,00

Definice Priorit Incidentů	Priorita	Definice
	Priorita 1 – Rozsáhlý incident	Služba nebo její část je celkově nedostupná a nedostupností jsou postiženi všichni uživatelé dané služby nebo významná skupina uživatelů. Dopad je vysoký, činnost dotčená daným incidentem nemůže být vykonána náhradním způsobem, jde o problém všech skupin uživatelů. Naléhavost je vysoká, neboť incident prokazatelně ohrožuje splnění termínu prováděné činnosti a neexistuje žádné náhradní řešení.
	Priorita 2 – Kritická	Služba nebo její část je mírně omezená a touto mírnou omezeností jsou postižení všichni uživatelé dané služby nebo významná skupina uživatelů. Incident omezuje uživatele, avšak nedochází k ohrožení termínu nebo existuje známé náhradní řešení.
	Priorita 3 – Vysoká	Ostatní incidenty.

Plánované odstávky
každou středu 22:00 - 5:00, maximálně na dobu 5 hodin nebo dle dohody s Objednatelem
Vymezující podmínky
Skupina uživatelů
pracovníci Zadavatele
Měření bude prováděno pouze pro produkční systémy, nebude prováděno pro systémy testovací a vývojové. Měření bude prováděno pouze v odsouhlasené provozní době postižené oblasti nebo prvku infrastruktury. Do doby vyřešení není započítáván čas čekání na součinnost Objednatele nebo Poskytovatele Objednatele.
Měření dostupnosti
Měření bude prováděno vyhodnocováním Trouble Ticketového (TT) a Dohledového systému. Dostupnost bude měřena jako podíl rozdílu celkové odsouhlasené provozní doby za sledované období a doby nedostupnosti služby, za níž nese odpovědnost Poskytovatel, k odsouhlasené provozní doby za sledované období vynásobené 100. Do odsouhlasené provozní doby za období se pro potřebu výpočtu dostupnosti promítnou plánované odstávky, pokud se uskutečnily v období zaručeného provozu služby. Dostupnost bude uvedena v %. **Dostupnost** = $(PD_{období} - N_{služby}) / PD_{období} * 100$ [%] Kde: $PD_{období}$ .... Odsouhlasená provozní doba za sledované období $N_{služby}$ ..... Doba úplné nedostupnosti služby ve sledovaném období, za níž odpovídá Poskytovatel Pro určení slevy za nedodržení dostupnosti je rozhodující jak „Maximální doba jednoho výpadku služby“, tak „Dostupnost služby měsíční“. Za každé překročení maximální doby jednoho výpadku služby je poskytnuta sleva v souladu se smlouvou v prioritě 1. Pokud se nedodržení „Maximální doby jednoho výpadku služby“ v hodnoceném období opakují, slevy se sčítají nezávisle na tom, zda byl parametr „Dostupnost služby měsíční“ splněn, či nikoliv. Uplatní-li se typ slev „Maximální doba jednoho výpadku služby“ v daném měsíci, neuplatňuje se sleva za nedodržení parametru „Dostupnost služby měsíční“ (zabránění dvojí penalizace z důvodu stejné příčiny). Při uplatnění slevy při překročení parametru „Dostupnost služby měsíční“ se výše slevy určuje dle smlouvy s prioritou 1.
Měření doby vyřešení
Měření bude prováděno vyhodnocováním Trouble Ticketového (TT) a Dohledového systému.

Dostupnost bude měřena jako podíl rozdílu celkové odsouhlasené provozní doby za sledované období a doby nedostupnosti služby, za níž nese odpovědnost Poskytovatel, k odsouhlasené provozní doby za sledované období vynásobené 100. Do odsouhlasené provozní doby za období se pro potřebu výpočtu dostupnosti promítnou plánované odstávky, pokud se uskutečnily v období zaručeného provozu služby. Dostupnost bude uvedena v %.

Dostupnost = (PDobdobí - Nslužby) / PDobdobí * 100 [%]

Kde: PDobdobí .... Odsouhlasená provozní doba za sledované období
Nslužby... Doba úplné nedostupnosti služby ve sledovaném období, za níž odpovídá Poskytovatel

Pro určení slevy za nedodržení dostupnosti je rozhodující jak „Maximální doba jednoho výpadku služby", tak „Dostupnost služby měsíční".

Za každé překročení maximální doby jednoho výpadku služby je poskytnuta sleva v souladu se smlouvou v příslušné prioritě.

Pokud se nedodržení „Maximální doby jednoho výpadku služby" v hodnoceném období opakují, slevy se sčítají nezávisle na tom, zda byl parametr „Dostupnost služby měsíční" splněn, či nikoliv. Uplatní-li se typ slev „Maximální doba jednoho výpadku služby" v daném měsíci, neuplatňuje se sleva za nedodržení parametru „Dostupnost služby měsíční" (zabránění dvojí penalizace z důvodu stejné příčiny). Při uplatnění slevy při překročení parametru „Dostupnost služby měsíční" se výše slevy určuje dle Smlouvy s prioritou 1.

Měření doby vyřešení
Měření bude prováděno vyhodnocováním Trouble Ticketového (TT). Plnění parametru „Doba vyřešení" v procentech bude vypočteno jako podíl rozdílu všech nahlášených incidentů dané priority a počtu porušených incidentů dané priority za sledované období k počtu všech incidentů dané priority za sledované období vynásobené 100.
Měření a vyhodnocení provádí Poskytovatel a předává ho Objednateli.

Doba vyřešení v %:

Doba vyřešení = (PI - PNI) / PI * 100 [%]

Kde: PI..... Počet nahlášených incidentů (servisních požadavků) dané priority ve sledovaném období

PNI..... Počet nevyřízených incidentů (servisních požadavků) dané priority ve stanovené době vyřešení ve sledovaném období

3.3 Služba provozu Call Centra – KL003

Kód služby	KL003
Název služby	**Služba provozu Call Centra**
Cíl služby	Cílem služby je zajistit jednotný systém správy požadavků, incidentů, problémů a změn a jejich monitoring, vyhodnocování a reporting
Popis služby	Service Desk V rámci této služby budou poskytovány činnosti související s provozem jednoho kontaktního místa (single point of contact-SPOC) pro uživatele služeb aplikačního provozu a pro uživatele služeb virtuální platformy dalších aplikací, technického provozu ICT služeb a podpůrných služeb včetně provozu troubleticketovacího systému. Toto kontaktní místo bude dostupné na bezplatné Zelené lince, emailové adrese a prostřednictvím tiketovacího nástroje Poskytovatele a bude zajištěno operátorským zabezpečením ze strany Poskytovatele. Na definovanou Zelenou linku nebo emailovou adresu nebo prostřednictvím tiketovacího nástroje budou hlášeny veškeré incidenty, požadavky a problémy uživatelů aplikačního provozu a kontaktních osob pro služby virtuální infrastruktury. V případě nejasností se stanovením priority incidentu je Poskytovatel povinen konzultovat s Objednatelem (zadavatelem incidentu) správnou hodnotu priority. V případě nesouladu stanovení priority Poskytovatelem s KL má Objednatel právo požadovat správné nastavení priority. Poskytovatel je pak povinen s touto prioritou pracovat tak, jako by byla nastavena od samého počátku. Služba Service desk bude zajišťovat a podporovat následující činnosti: • řízení životního cyklu Incidentu • řízení životního cyklu Požadavku • řízení životního cyklu Požadavku na změnu • komunikace s Objednatelem • reporting • součinnost se 3. stranami • tvorba a údržba provozní dokumentace týkající se služby Service Desk Řízení životního cyklu Incidentu • plnění role 1. úrovně podpory v procesu Incident Managementu, kam především patří: o příjem Incidentů o analýza Incidentů o kategorizace Incidentů o prvotní řešení incidentů, je-li k dispozici databáze známých chyb o předávání řešení incidentů na 2. úroveň podpory (dle metodiky ITIL) o sledování a průběžná kontrola řešení Incidentů

o ověřování vhodnosti řešení u uživatele
o uzavírání Incidentů

• Koordinace 2. a 3. úrovně podpory v procesu Incident Managementu (dle metodiky ITIL)
• Zajišťování funkční či hierarchické eskalace

Řízení životního cyklu Požadavku
• identifikace požadavku
• předání požadavku na řešitele
• sledování a průběžná kontrola řešení požadavku
• ověřování řešení u uživatele
• uzavírání požadavku

Řízení životního cyklu Požadavku na změnu
• příjem a evidence Požadavku na změnu
• předávání Požadavků na změnu na vyjádření Metodickému oddělení Objednatele
• předávání Požadavků na změnu k realizaci Poskytovatelům
• sledování a průběžná kontrola plnění Požadavků na změnu

Komunikace s Objednatelem
• průběžná informovanost Objednatele o stavu vyřizování jimi hlášených incidentů, problémů a požadavků
• informování Objednatele a jeho uživatelů o plánovaných odstávkách systémů, o připravovaných změnách a dopadu těchto změn a odstávek.
• generování automatických hlášení prostřednictvím elektronické pošty na definované pracoviště Objednatele

Reporting
• Příprava standardních a zákaznických reportů

Součinnost se 3. stranami
• v rámci zajištění podpory 2. úrovně zabezpečovat komunikaci se 3. stranami v případě záručních oprav, řešení problémů či nestandardních požadavků na změny
• Komunikace se třetími stranami bude probíhat prostřednictvím emailu a telefonu.

Školení koncových uživatelů a 3. stran na užívání troubleticketovacího systému (max. 2x do roka).
Tvorba/udržování a poskytování dokumentace příručky troubleticketovacího systému Objednateli i 3. stranám

Poskytovatel se zavazuje dodržovat principy ITIL a je povinen zajistit účast expertů

	na jednání, pokud si je Objednatel vyžádá.
Dostupnost služby	Parametr dostupnosti služby je určován dobou reakce v časech zaručeného provozu služby s tím, že Dobou reakce se myslí čas, který uplyne od nahlášení Incidentu / Servisního požadavku Objednatelem do jeho přijmutí operátorem Service Desku vyjádřeným odesláním potvrzovací zprávy Servis Deskem mailem na adresu nahlašovatele Incidentu / Servisního požadavku. Do doby reakce se nezapočítává čas mimo „Rozsah zaručeného provozu služby"

Služba	Příjem	Rozsah zaručeného provozu služby
Příjem kontaktů e-mailem	7x24	Pracovní dny 7:00-18:00
Příjem telefonických kontaktů	Pracovní dny 7:00-18:00	Pracovní dny 7:00-18:00

Mimo „Rozsah zaručeného plnění provozu služby" zajistí Poskytovatel telefonickou linku dostupnou v režimu 7x24, kterou budou moci i v době mimo „Rozsah zaručeného plnění provozu služby" využít provozovatelé aplikací a Objednatel v případě problémů s provozem infrastruktury. Telefonní číslo této linky předá Poskytovatel Objednateli ke dni účinnosti této smlouvy a o případných změnách bude Objednatele informovat minimálně s měsíčním předstihem. Pro tuto linku neplatí parametry Dostupnosti a SLA uváděné následně v tomto katalogovém listu.

Dostupnost služby měsíční: 98%.

Maximální doba jednoho výpadku: 120 minut.

Maximální počet uživatelů, kterým jsou poskytovány služby dle katalogových listů: až 5 000 uživatelů. Měření dostupnosti bude prováděno vyhodnocováním Trouble Ticketového (TT) a Dohledového systému.

Dostupnost se měří dohromady za přijaté e-maily i telefonické kontakty. Dostupnost bude měřena jako podíl rozdílu celkového rozsahu zaručeného provozu služby doby za sledované období a doby nedostupnosti služby v tomto období, za níž nese odpovědnost Poskytovatel, k celkovému rozsahu zaručeného provozu služby doby za sledované období vynásobené 100. Do celkového rozsahu zaručeného provozu služby doby za sledované období se pro potřebu výpočtu dostupnosti promítnou i plánované odstávky, pokud se uskutečnily v období zaručeného provozu služby. Dostupnost bude uvedena v %.

Dostupnost = (PDobdobí - Nslužby) / PDobdobí * 100 [%]

Kde:

PDobdobí .... celkový rozsah zaručeného provozu služby doby za sledované období Nslužby Doba úplné nedostupnosti služby ve sledovaném období, za níž odpovídá Poskytovatel

SLA	U 90% nahlášených Incidentů / Servisních požadavků za sledované období musí být Doba reakce: Pro období: pracovní dny 7:00-18:00 (pracovní doba) • 15 minut pro nahlášení telefonem; • 30 minut pro nahlášení e-mailem. Pro období mimo pracovní dobu: • Následující pracovní den do 7:30 hodin Měření Doby reakce bude prováděno vyhodnocováním Trouble Ticketového (TT) a Dohledového systému. Plnění parametru „Doba reakce" v procentech bude vypočteno jako podíl rozdílu všech nahlášených Incidentů / Servisních požadavků za sledované období a počtu překročených Dob reakce za sledované období k počtu všech nahlášených Incidentů / Servisních požadavků za sledované období vynásobené 100. Měření a vyhodnocení předkládá Objednateli Poskytovatel. Plnění v %: **Plnění** = (PI - PNI) / PI * 100 [%] Kde: P I . . počtu všech nahlášených Incidentů / Servisních požadavků za sledované období PNI počet překročených Dob reakce za sledované období Při výpadku služby je Poskytovatel povinen bezodkladně informovat Objednatele o výpadku, o obnovení služby; dále je Poskytovatele povinen: V pracovní dny v čase od 7:00 do 18:00 do 60 minut od výpadku písemně informovat Objednatele o stavu a zjištěných příčinách/důsledcích; do 24 hodin od obnovení služby podat komplexní písemnou zprávu o příčinách a důsledcích výpadku i o nápravných opatřeních. V ostatním čase pak do 9:00 hodin následujícího pracovního dne po výpadku písemně informovat Objednatele o stavu a zjištěných příčinách/důsledcích a do 24 hodin od této informace podat komplexní písemnou zprávu o příčinách a důsledcích výpadku i o nápravných opatřeních.
Možnost plánovaných odstávek	Mimo pracovní dobu a po dohodě s Objednatelem.

3.4 Služba převzetí provozu – KL004

Kód služby	KL004
Název služby	**Služba převzetí provozu**
Cíl služby	Cílem služby je zajistit u Poskytovatele potřebnou infrastrukturu nutnou k poskytování služeb KL001-KL003 Poskytovatelem a zajistit migraci provozu aplikací na tuto Poskytovatelovu infrastrukturu z infrastruktury předchozího Poskytovatele služeb
Popis služby	Služba musí zajistit migraci, která se skládá: 1. Z přípravného období, ve kterém musí Poskytovatel zajistit vytvoření SW a HW prostředí pro následný provoz služeb v rozsahu a kvalitě, které vyžaduje provoz KL 001 až KL003. 2. Z návrhu reálného harmonogramu přechodu prostředí, aplikací, licencí a dalších komponent nezbytných pro provoz služeb, který bude realizován dle těchto zásad: a. Harmonogram přechodu musí být předložen ke schválení a připomínkám Objednateli do 30 kalendářních dnů od účinnosti Smlouvy. Harmonogram musí počítat s oznámením požadavků na Poskytovatele podpory provozu aplikací (součinnost/změny) minimálně 14 kalendářních dní předem, nedohodne-li se Poskytovatel s Objednatelem na kratším termínu. b. Pokud budou přechody rozděleny do dílčích přechodů realizovaných v různých termínech, bude pro každý takový dílčí přechod stanoven dílčí harmonogram. c. Harmonogram (-y) a jejich případné úpravy budou schvalovány Objednatelem. d. Součinnost Poskytovatele podpory provozu aplikace bude spočívat pouze v otestování úspěšnosti přechodu, v konzultaci, případně ve změně IP adres (bude-li to nezbytně nutné). e. Součástí přechodu (dílčího přechodu) musí být testovací scénář pro provozovatele aplikací (aplikace). f. Každá migrace musí obsahovat možnost návratu do výchozího stavu v termínu stanoveném pro migrační okno za situace, kdy se migraci nepodaří realizovat tak, aby migrovaná aplikace byla schopna bezproblémového provozu v novém prostředí. g. Každému přechodu musí předcházet test přechodu, resp. test dílčího přechodu. Požadavky na opakované testování Poskytovatelem podpory provozu aplikace z důvodu problémů způsobených Poskytovatelem nebudou Objednatelem Poskytovateli hrazeny a vznikne-li nárok na úhradu ze strany Poskytovatele podpory provozu aplikace, musí být vypořádány Poskytovatelem, rovněž bez nároku na jejich refundaci Objednatelem. Obdobně se bude postupovat v situaci chybného zadání požadavku na úpravy aplikace (změny IP adres) z důvodu migrace provozu k Poskytovateli.

	3. Přechod aplikací do cílového stavu má stanovenu maximální dobou odstávky: 36 hodin o víkendu 4. Provoz již převedeného (-ných) systému (-ů) do doby plného ukončení tohoto KL s SLA stanovenými v KL001-KL003. 5. Spolupráci se stávajícím (současným) provozovatelem IT infrastruktury 6. Poskytovatel musí umožnit kontrolu ze strany Objednatele v rozsahu stanoveném Smlouvou, a to i za využití 3. stran, které Objednatelem kontrolou pověří. 7. Poskytovatel musí na vlastní náklady veškeré nezbytné licence k převzetí služby.
Rozsah zaručeného provozu služby	Kompletní realizace do termínů stanovených Smlouvou
SLA	Splnění v termínech Smlouvy; u již zmigrovaných částí se SLA řídí SLA v rozsahu příslušného katalogového listu, který se dotčené aplikace týká, a to až do ukončení této služby.
Možnost plánovaných odstávek	Viz popis služby

3.5 Služba předání provozu – KL005

Kód služby	KL005
Název služby	**Služba předání provozu**
Cíl služby	Cílem služby je zajistit migraci provozu aplikací na infrastruktuře provozovaných Poskytovatelem k jinému Poskytovateli služeb nad rámec povinností dle Smlouvy - Exit plán
Popis služby	Služba musí zajistit nad rámec povinností obsažených v ostatních katalogových listech, resp. Dle Smlouvy - Exit plán součinnost tak, aby nedošlo k ohrožení provozu předávaných agend. Služba je určena zajištění součinnosti Poskytovatele na předání služeb v oblastech, které nelze v okamžiku podpisu této smlouvy přesně popsat a je zaměřena především na tyto oblasti: 1. Poskytnout novému provozovateli infrastruktury veškeré potřebné informace 2. Umožnit migraci dat, konfigurací, licencí i aplikací a spolupracovat s Objednatelem a 3. stranami tak, aby nedocházelo k zbytečným zpožděním, výpadkům a odstávkám.
Rozsah zaručeného provozu služby	Kompletní realizace do termínů stanovených smlouvou
SLA	Splnění v termínech a rozsazích Smlouvy
Možnost plánovaných odstávek	N/A

3.6 Služba na vyžádání – KL006

Kód služby	KL006
Název služby	**Služba na vyžádání**
Cíl služby	Cílem této služby je umožnit realizaci požadavků Objednatele v závislosti na potřebách provozovaných aplikací, bezpečnosti a technologickém vývoji
Popis služby	Služba umožňuje zajistit činnosti nad rámec katalogových listů KL001- KL005 v závislosti na potřebách Objednatele, které Objednatel nemohl předvídat, resp. přesně popsat v okamžiku uzavření Smlouvy. Jedná se o činnosti, které souvisejí se službami popsanými v KL001-KL005 a které nelze především z důvodů technologických, bezpečnostních či z důvodů požadavku odpovědnosti za SLA zajistit jiným Poskytovatelem. Služby na vyžádání se objednávají po dohodě Poskytovatele a Objednatele. Poskytovatel předloží Objednateli na základě požadavků Objednatele nabídku, na jejímž základě Objednatel vystaví objednávku. V objednávce bude stanoven též termín realizace, SLA, cena a akceptační kritéria. Pro stanovení ceny služeb na vyžádání se využije cena v místě a čase obvyklá pro danou činnost, avšak nejvýše do hodnoty stanovené pro tento KL ve Smlouvě.
Rozsah zaručeného provozu služby	Dle dohody stanovené objednávkou
SLA	Splnění v termínech a rozsazích Smlouvy
Možnost plánovaných odstávek	N/A

4 Seznam zkratek

ISPOP	Informační systém plnění ohlašovacích povinností
EnviHELP	Environmentální helpdesk
CR	Česká republika
DB	Databáze
DC	Datové centrum
DPH	Daň z přidané hodnoty
HZS	Hasičský záchranný systém
IS	Informační systém
L2	2. datová vrstva OSI modelu (Open System Interconnection Reference Model)
MS	Společnost Microsoft
OS	Operační systém
RV	Řídící výbor
ACS	Access Control System
ASM	Automatic Storage Management
CCTV	Closed Circuit Television
CPU	Central Processing Unit
EPS	Elektronický protipožární systém
EZS	Elektronická zabezpečovací signalizace
ERP	Enterprise Resource Planning System
HR	Human Resources
HVAC	Heating, ventilating and air conditioning
HW	Hardware
ICT	Information and Communication Technologies
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network

LDAP	Lightweight Directory Access Protocol
MSCS	Microsoft Cluster Server
MBR	Managed Backup and Restore
MDS	Služba Managed Data Storage
OTRS	Opensource Ticket Request System
RAC	Real Application Cluster
RAM	Random Access Memory
SAN	Storage Area Network
SD	Service Desk
SLA	Service Level Agreement
SPOC	Single Point Of Contact
SPLA	Services Provider License Agreement
SQL	Structured Query Language
SSL	Secure Sockets Layer
SW	Software
TT	Trouble Ticket
VESDA	Very Early Smoke Detection Apparatus
VIP	Virtual IP Address
VLAN	Virtual Local Area Netwok
VPN	Virtual Private Network

5 Technologická platforma ISPOP a EnviHELP

Popis poptávané technologické platformy je uveden v tabulkách níže. Jsou požadovány dvě geograficky oddělené lokality. Součástí poptávky jsou služby zálohování, networking, firewall, load balancing, VPN.

Virtuální servery

Lokalita	Název serveru	vCPU	Paměť [GB]	Disk 300 IOPS (výkon min. 2 IOPS na každý GB prostoru) [GB]	OS
Lokalita č.1	ISPOP-1	8	64	150	CentOS 7
	ISPOP-BG	8	64GB	50	CentOS 7
	ADOBE-1	8	32	80	RHEL 5.5
	INFRA	2	4	20	CentOS 7
	MONITOR	2	2	50	CentOS 6
	ENV-1	8	32	150	CentOS 7
	TOVEK-1	4	8	70	SuSe 11

Lokalita	Název serveru	vCPU	Paměť [GB]	Disk 300 IOPS (výkon min. 2 IOPS na každý GB prostoru) [GB]	OS
Lokalita č.2	ISPOP-2	8	64	150	CentOS
	ADOBE-2	8	32	80	RHEL 5.5
	DEV-TEST	8	64	300	CentOS
	TOVEK-TEST	2	4	50	SuSe 11

Fyzické servery (dedikované)

Lokalita	Název serveru	CPU [počet]	CPU [jader]	Paměť [GB]	Disk 700 IOPS (výkon min. 5 IOPS na každý GB prostoru) [GB]	Disk 1000 IOPS (výkon min. 10 IOPS na každý GB prostoru) [GB]	OS
Lokalita č.1	DB-1	1	8	128	150GB OS+DB binarky	6x300GB DB data - sdílený 6x100GB DB logy- sdílený 6x2GB – DB OCR logu - sdílený	Oracle Linux 7
Lokalita č.2	DB-2	1	8	128	150GB OS+DB binarky		Oracle Linux 7