


## Dodatek č. 2

ke smlouvě „Poskytování služeb provozu infrastruktury pro informační systémy Ministerstva dopravy“, ev. č. S-8-330/2017, ze dne 16. 5. 2017 (dále jen „Smlouva“)

(dále jen „Dodatek“)

### Smluvní strany:


#### 1. Česká republika – Ministerstvo dopravy

se sídlem: nábřeží L. Svobody 1222/12, 110 15 Praha 1  
zastoupená: Mgr. Jakubem Kopřivou, náměstkem ministra  
IČO: 66003008  
DIČ: CZ66003008  
Bankovní spojení: 

(dále jen „Objednatel“)

a

#### 2. O2 IT Services s.r.o.

se sídlem: Za Brumlovkou 266/2, 140 00 Praha 4  
zastoupená: Ing. Janem Bechyněm a Mgr. Janem Hruškou, jednatelem společnosti  
zapsaná: v obchodním rejstříku Městského soudu v Praze, oddíl C, vložka 223566  
IČO: 02819678  
DIČ: CZ02819678  
Bankovní spojení: 

(dále jen „Dodavatel“)

### Čl. I Úvodní ustanovení

1. V návaznosti na změny informačních systémů Objednatel provozovaných na infrastruktuře poskytované Dodavatelem na základě Smlouvy Objednatel v souladu s § 222 odst. 5 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „Zákon“), požaduje změny parametrů poskytovaných Služeb. Tyto změny nelze technologicky zajistit prostřednictvím jiného dodavatele, protože technologie, licence a další služby nezbytné k provozu informačních systémů jsou bezprostředně spojeny s předmětem plnění dle Smlouvy. Realizace

změn, které jsou předmětem Dodatku, prostřednictvím jiného dodavatele tedy není možná především z technických důvodů spočívajících zejména v požadavcích na slučitelnost a interoperabilitu se stávajícími Službami zajišťovanými na základě Smlouvy. Změna dodavatele by způsobila výrazné a neodůvodněné navýšení nákladů a dále značná rizika provozu informačních systémů zařazených zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a navazujících vyhlášek do kategorie KIS (Kritická infrastruktura státu) a VIS (významný informační systém). Hodnota této změny, ani v součtu všech změn dle § 222 odst. 5 a 6 Zákona, nepřekročí Zákonem stanovený limit z původní hodnoty závazku.

2. Smluvní strany se dohodly v souladu s odst. 14.1. Smlouvy na uzavření Dodatku, kterým se Smlouva mění způsobem a v rozsahu uvedeném v čl. II Dodatku.

## **Čl. II. Předmět Dodatku**

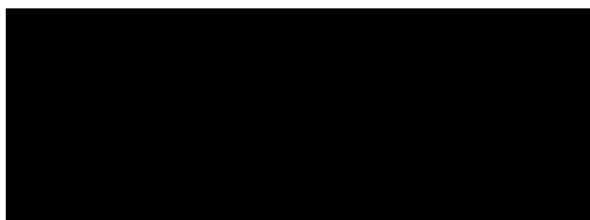
1. Smluvní strany se dohodly na změně Přílohy č. 2 Smlouvy. Příloha č. 2 Smlouvy se zrušuje a nahrazuje se novou Přílohou č. 2, která je nedílnou součástí Dodatku jako jeho Příloha č. 1.
2. Smluvní strany se dále dohodly na změně Přílohy č. 4 Smlouvy. Příloha č. 4 Smlouvy se zrušuje a nahrazuje se novou Přílohou č. 4, která je nedílnou součástí Dodatku jako jeho Příloha č. 2.
3. Celkový rozsah Služeb za období platnosti Smlouvy stanovený v odst. 3.13 Smlouvy se nemění a nesmí překročit hodnotu 275 000 000,- Kč bez DPH. Dodavatel je dle odst. 3.13 Smlouvy povinen upozornit písemně a bezodkladně Objednatele při vyčerpání 75 % sjednaného limitu.
4. Změna parametrů služeb bude provedena podle pokynů Objednatele do termínu 1. 3. 2019. Od termínu akceptace realizace změn bude Objednatel za služby uvedené v Příloze č. 1 Dodatku platit ceny uvedené v Příloze č. 2 Dodatku. Nebude-li dnem rozhodným pro změnu výše plateb začátek měsíce, provede se úhrada za daný měsíc v poměrné výši podle počtu dní platnosti původní a nové cenové specifikace.

## **Čl. III. Závěrečná ustanovení**

1. Dodatek nabývá platnosti dnem jeho podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv.
2. Ostatní ustanovení Smlouvy nejsou Dodatkem dotčena a zůstávají beze změny.
3. Dodatek je vyhotoven v 5 (slovy: pěti) vyhotoveních s platností originálu, z nichž 3 (slovy: tři) obdrží Objednatel a 2 (slovy: dvě) obdrží Dodavatel.
4. Dodavatel bere na vědomí a souhlasí s tím, že Dodatek Objednatel uveřejní v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.

5. Smluvní strany prohlašují, že si Dodatek přečetly, s jeho zněním souhlasí a na důkaz pravé a svobodné vůle připojují níže své podpisy.
6. Nedílnou součástí Dodatku jsou následující přílohy:
  - Příloha č. 1: Příloha č. 2 Smlouvy - Katalogové listy
  - Příloha č. 2: Příloha č. 4 Smlouvy - Specifikace ceny

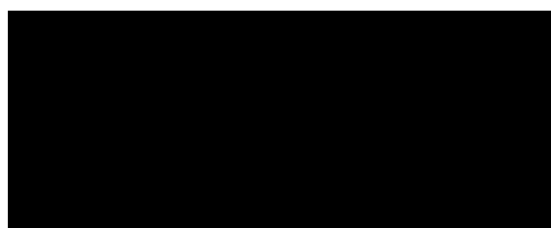
V Praze dne 27. 2. 2019



**Česká republika – Ministerstvo dopravy**

Mgr. Jakub Kopřiva  
náměstek ministra

V Praze dne 25. 2. 2019



**O2 IT Services s.r.o.**

Ing. Jan Bechyně  
jednatel za O2 IT Services s.r.o.

a

Mgr. Jan Hruška  
jednatel za O2 IT Services s.r.o.

**Katalogové listy**

**„Poskytování služeb provozu infrastruktury pro informační systémy  
Ministerstva dopravy“**

## Obsah:

Pravidla při aplikaci hodnocení SLA .....	3
1 Služba bezpečnostní politiky – KL001.....	4
2 Služba technického provozu a poskytování virtuální infrastruktury – KL002.....	13
3 Služba provozu CRŘ – KL003.....	35
4 Služba provozu Call Centra– KL004 .....	39
5 Služba převzetí provozu – KL005 .....	44
6 Služba předání provozu – KL006.....	46
7 Služba na vyžádání – KL007.....	47
8 SEZNAM ZKRATEK.....	48

## **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-passive), 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 Dodavatelem a Dodavatel nemohl toto neplnění SLA nijak ovlivnit.

## 1 Služba bezpečnostní politiky – KL001

Kód služby	<b>KL001</b>
Název služby	<b>Služba bezpečnostní politiky</b>
Cíl služby	Cílem služby je zajištění zvýšené bezpečnosti provozu poskytovaných infrastrukturních služeb.
Popis služby	<p><b>Obecné požadavky</b> Řízení bezpečnosti zahrnuje tyto ICT oblasti:</p> <ul style="list-style-type: none"> <li>• datové centrum (DC)</li> <li>• komunikační infrastrukturu (včetně komunikace s Centrálním místem služeb (CMS))</li> <li>• serverovou a datovou infrastrukturu</li> <li>• virtuální infrastrukturu – tím je myšleno nejméně datové centrum (fyzicky), komunikační infrastruktura (sítě vč. aktivních prvků), servery (fyzické vč. komponent, racky, chasis, switche, virtualizace a operační systémy, systémové služby (zejména zálohování, updaty)</li> <li>• Systémové služby – zajišťují spolupráci mezi jednotlivými systémy, zajišťují bezpečný přístup ke službám a aplikacím apod.</li> </ul> <p>Dodavatel 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.</p> <p>Dodavatel zajistí služby 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 i v návaznosti na změny prováděné v ostatních katalogových listech. Dodavatel se musí též řídit pravidly příslušné části bezpečnostní dokumentace Ministerstva dopravy.</p> <p>Dodavatel provádí opatření v následujících oblastech:</p> <ul style="list-style-type: none"> <li>• <b>Organizační a personální bezpečnost</b> <ul style="list-style-type: none"> <li>• Dodavatel musí splňovat podmínku své bezúhonnosti i bezúhonnosti osob zajišťujících plnění Smlouvy po celou dobu její platnosti.</li> <li>• Dodavatel 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.</li> <li>• Dodavatel zajistí po celou dobu poskytování služeb efektivní provoz svého systému řízení bezpečnosti informací podle obecně uznávané metodiky ISO/IEC 27 001 pro poskytované služby.</li> <li>• Dodavatel zajistí realizaci změn v přístupových právech fyzických (do objektů) i logických (k systémovým komponentám) v důsledku změn v zařazení pracovníků, kteří měli/mají přístup.</li> <li>• Dodavatel 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.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"><li>• Seznamování osob s provozním řádem DC a poučení osob s právem přístupu do DC provádí Dodavatel opakovaně a vede o tom evidenci.</li><li>• Dodavatel vede evidenci vstupů osob do DC.</li><li>• Dodavatel poskytne evidenci vstupů, seznamování osob s provozním řádem a s poučením na vyžádání Objednateli (formou nahlédnutí na místě).</li><li>• Dodavatel po dobu přítomnosti osob třetích stran v DC zajistí jejich trvalé doprovázení pracovníky Dodavatele, kteří byli seznámeni s provozním řádem DC a poučení o svých povinnostech.</li><li>• Dodavatel poskytne spojení na kontaktní fyzické osoby pro podporu řešení problémů s provozem informačních systémů (IS) Objednatele. Dodavatel je povinen spolupracovat při řešení problémů (bezpečnostních) s dodavateli aplikací a ostatních programových komponent (třetími stranami).</li><li>• Dodavatel 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.</li><li>• Dodavatel musí udržovat aktuální vlastní bezpečnostní směrnice a na vyžádání je Objednateli předložit minimálně k nahlédnutí.</li><li>• Dodavatel musí mít nastaveny efektivní a evidované procesy Change a Incident Managementu a na vyžádání je předložit oprávněným pracovníkům Ministerstva dopravy minimálně k nahlédnutí.</li><li>• Dodavatel 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 Dodavatel povinen tyto změny předložit MD vždy k 31. prosinci, po dobu platnosti Smlouvy, a rovněž ke dni ukončení jeho aktivit plynoucích ze Smlouvy se Objednatelem.</li><li>• <b>Fyzická bezpečnost</b><ul style="list-style-type: none"><li>• Dodavatel zajistí umístění prostor DC na území České republiky, plně podléhající legislativě České republiky, mimo zátopovou oblast, mimo bezprostřední dosah produktovodů a jinak kritických míst.</li><li>• Dodavatel umístí hardware pro provoz infrastruktury Objednatele (např. servery, disková pole či switche), do uzamykatelných skříní s řízeným přístupem a s chráněnými přístupy ze všech stran (nebo s vyšší úrovní zabezpečení přístupů k hardwaru užívaného pro Objednatele).</li><li>• Dodavatel umožní využít i racky třetích stran nebo ve spolupráci s třetími stranami zajistí provoz hardware třetích stran původně umístěných v racku třetí strany tak, aby se zaslíbené podmínky provozu třetí strany vůči Objednateli neměnily.</li><li>• Dodavatel zajistí elektronickou zabezpečovací signalizaci (EZS) napojenou na kamerový systém (CCTV) a systém kontroly vstupu (ACS).</li></ul></li></ul>
--	---



	<ul style="list-style-type: none"> <li>• Dodavatel zajistí ochranu proti násilnému fyzickému vniknutí do prostor DC z prostor mimo DC.</li> <li>• Dodavatel zajistí 24 hodinovou ostrahu s připojením systému EZS k pultu centralizované ochrany PČR, bezpečnostní agentury či ekvivalentní formu dohledu.</li> <li>• Dodavatel zajistí CCTV způsobem, že monitoruje vstup oprávněných osob do datového sálu; Dodavatel zajistí, aby tento monitoring byl v souladu s platnou legislativou.</li> <li>• Dodavatel zajistí systém perimetrické ochrany datového sálu (tzn. Dodavatel preventivně zjišťuje bezpečnostní incidenty a efektivně je řeší ještě mimo vlastní sál DC – např. zajištěním ochrany celého objektu, kde je datový sál provozován).</li> <li>• Dodavatel 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).</li> <li>• Dodavatel zajistí propojení systému EPS s pultem centralizované ochrany Hasičského záchranného systému (HZS) nebo bezpečnostní agentury.</li> <li>• Dodavatel zajistí monitoring teploty sálu a jednotlivých racků se vzdáleným přístupem k těmto informacím pro oprávněné osoby.</li> <li>• Dodavatel zajistí ochranu proti vytopení DC zevnitř, formou napojení na EZS s neustálým dohledem.</li> <li>• Dodavatel zajistí detekci zaplavení sálu.</li> <li>• Dodavatel zajistí režim ostrahy a připojení výše uvedených systémů v režimu 24x7.</li> <li>• Dodavatel zajistí způsob ostrahy znemožňující fyzický přístup nepovolaným osobám.</li> <li>• Dodavatel zajistí řízený přístup k systémovým komponentám a to minimálně s ověřením ostrahou a kartou.</li> <li>• Dodavatel 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.</li> <li>• Dodavatel umožní Objednateli a jím určeným osobám přístup k záznamům CCTV a logům EZS a EPS minimálně k nahlédnutí.</li> <li>• Dodavatel zajistí nemožnost změny pořízených záznamů a logů.</li> <li>• Dodavatel zajistí provozní podmínky zařízení pro poskytované služby dle doporučení výrobce.</li> </ul> <ul style="list-style-type: none"> <li>• <b>Provozní bezpečnost</b> Dodavatel DC zajistí splnění požadavků kategorie TIER III DC (lze využít certifikát TIER III DESIGN dle UPTIME institute nebo předložit jiné důvěryhodné dokumenty, které dokládají splnění požadavků), kde jsou požadovány vlastnosti zejména: <ul style="list-style-type: none"> <li>• Zajistit redundanci všech klíčových prvků: <ul style="list-style-type: none"> <li>○ Zajistit redundanci napájecích okruhů, tj. napájení nejméně ze dvou rozdílných směrů.</li> <li>○ Zajistit redundanci síťových přípojek tj. připojení k nadřazené síťové infrastruktuře nejméně ze dvou rozdílných směrů s tím,</li> </ul> </li> </ul> </li> </ul>
--	--

	<p>že trasy vedení síťového spojení nejsou totožné s trasami vedení napájení.</p> <ul style="list-style-type: none"> <li>○ Zajistit redundanci aktivních síťových prvků (přepínačů a směrovačů) přímo v DC.</li> <li>○ Zajistit redundanci ventilace.</li> <li>○ Zajistit redundanci chlazení.</li> <li>○ Zajistit redundanci zdrojů (napájení) serverů: fyzické servery obsahují nejméně dva zdroje s tím, že zdroje jsou napojeny každý na jiný okruh napájení.</li> </ul> <ul style="list-style-type: none"> <li>● Zajistit náhradní napájení pro provoz technologií Objednatele a souvisejících technologií DC nejméně na 24 hod.</li> <li>● Zajistit pravidelné kontroly funkce všech záložních napájecích zdrojů nejméně jednou ročně a vede o tom zápisy, které je schopen na vyžádání předložit.</li> <li>● Zajistit pravidelnou údržbu hardware a vede o tom zápisy, které je schopen na vyžádání předložit.</li> <li>● Zajistit lokální zdroj přesného času, který využijí všechny instalované prvky v DC. Zajistí synchronizaci času lokálního zdroje času nejméně jednou denně.</li> <li>● Zajistit auditovatelný dohled nad Objednatelem požadovanými systémy minimálně po dobu Objednatelem požadovanou a na vyžádání o něm poskytne informace Objednateli.</li> <li>● Instalované technologie budou monitorovány Dodavatelem. Dodavatel 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.</li> <li>● Zajistit striktní oddělení jednotlivých OS způsobem využívajícím virtualizační prostředí.</li> <li>● 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.</li> <li>● Umožnit využití dedikovaného hardware pro instalaci software (operační systém, databáze.)</li> <li>● Bezpečnostní dohled a správa bude provozována z jednoho místa, které má záložní řešení.</li> <li>● Zajistit pravidelné provádění skenů externí a interní zranitelnosti nejméně jednou ročně a při významné změně systémových komponent. Na vyžádání poskytne informaci o provedených testech.</li> <li>● Umožnit po vzájemné dohodě provádění skenů externí a interní zranitelnosti na požadavek Objednatele nebo jím určené osoby. Rozsah součinnosti dodavatele nepřekročí 3 člověkodny za rok.</li> <li>● Používat techniky detekce a prevence narušení v souladu s oborovými standardy, udržovat je aktualizované.</li> <li>● Zajistit mechanismus detekce změn konfigurace systémových komponent a řízenou reakci na tyto změny, která zahrnuje informování Objednatele.</li> <li>● Zajistit trvalý vzdálený přístup Objednatele k systémovým logům pro jednotlivé komponenty infrastruktury souvisejících s poskytovaným</li> </ul>
--	--

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**

- Dodavatel 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 (dodavatelům aplikací) uživatelský přístup za účelem konfigurace ověřování a provádění ověřování.
- Dodavatel umožní využít pro stávající systémy definované touto Smlouvou nástroj pro řízení přístupových oprávnění. Umožní Objednateli a třetím stranám (dodavatelům aplikací) uživatelský přístup za účelem konfigurace ověřování a provádění ověřování.
- Dodavatel zajistí nástroj pro ochranu před škodlivým kódem na úrovni perimetru DC, jeho pravidelnou aktualizaci a automatizovaný sběr údajů.
- Dodavatel 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.
- Dodavatel zajistí nástroj pro zaznamenávání činností komponent vztahujících se k předmětu plnění zaznamenaných do systémových logů způsobem, který zaznamenává nejméně:
  - přihlášení a odhlášení uživatelů a administrátorů,
  - činnosti provedené administrátory,
  - činnosti vedoucí ke změně přístupových oprávnění,
  - neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
  - zahájení a ukončení činností systémů,
  - automatická varovná nebo chybová hlášení systémů,
  - přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností,
  - použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

- Dodavatel zajistí 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 Nástroj pro sběr a vyhodnocování kybernetických bezpečnostních událostí (SIEM). Nástroj zajistí:
  - integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí, včetně činnosti administrátorů a případně koncových uživatelů, z informačních systémů Ministerstva dopravy (výchozí rozsah plnění je stanoven plněním pro servery a na nich provozované aplikace stanovené v KL002 a KL003),
  - bezodkladné poskytování informací Objednateli a jím určených bezpečnostní rolích o detekovaných kybernetických bezpečnostních událostech,
  - nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování Objednatele, resp. jím určených bezpečnostních rolí, příp. po dohodě se Objednatelem umožní Objednateli zobrazování včasného varování na centrální grafické konzoli Nástroje, a to min. v úrovni agregovaných manažerských informací,
  - Dodavatel zajistí sám anebo v příp. spolupráci se Objednatelem, resp. i se správcí ostatních informačních systémů aktualizaci nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování,
  - Dodavatel zajistí využívání informací v rámci plnění této Smlouvy, které jsou připraveny nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření informačních systémů,
  - Dodavatel zajistí, aby svou činností současně nijak nemodifikoval žádný z informačních systémů kritické informační infrastruktury ani žádný z významných informačních systémů.
- Umožní po dohodě s Objednatelem nasazení nástroje na případné další důležité informační systémy Objednatele provozované na infrastruktuře Dodavatele.
- Dodavatel tak zajistí nástroj pro detekci kybernetických bezpečnostních událostí (IDS/IPS) na úrovni perimetru DC, určení jejich významu a dopadu a zahájení procesu reakce na ně, včetně jejich oznámení 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 a informování Objednatele. Umožní Objednateli a jím označeným subjektům vzdálený přístup pro čtení detekovaných kybernetických bezpečnostních událostí.
- Na žádost Objednatele Dodavatel poskytne podklady (logy) a spolupráci pro analýzu provozu/incidentů automatizovanými nástroji.
- Bezpečnostní dohled prostřednictvím SIEM zajistí zejména:

	<ul style="list-style-type: none"> <li>○ zaznamenávání činnosti infrastruktury (síťová infrastruktura, hardware, operační systémy, databáze, virtualizace, případně další), na které jsou provozovány informační systémy MD,</li> <li>○ zaznamenávání údajů o komunikaci informačních systémů MD na perimetru DC,</li> <li>○ zaznamenávání údajů činnosti informačních systémů MD na provozované infrastruktuře,</li> <li>○ detekci kybernetických bezpečnostních událostí na základě výše uvedených záznamů,</li> <li>○ upozornění na výskyt bezpečnostních událostí v reálném čase,</li> <li>○ podporu pro vyhodnocení a analýzu bezpečnostních událostí s cílem rozhodnout, zda jde o bezpečnostní incident, tj. událost, která znamená ohrožení bezpečnosti informačního systému MD.</li> </ul> <ul style="list-style-type: none"> <li>● Dodavatel umožní po dohodě s Objednatelem zasilání záznamů z jiných informačních systémů MD.</li> <li>● Dodavatel 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 činnosti informační infrastruktury a informačních systémů, jejich uživatelů a administrátorů; v případě nesouladu informuje Objednatele a jím vyznačené subjekty.</li> <li>● Dodavatel zajistí ochranu záznamů (logů) proti změně a neautorizovanému přístupu.</li> <li>● Dodavatel po vzájemné dohodě umožní externím subjektům provedení auditu informační bezpečnosti. Rozsah součinnosti dodavatele nepřekročí 3 člověkodny za rok.</li> <li>● Dodavatel zajistí zálohování dat způsobem, který zajistí bezpečné uchování záloh (proti fyzické destrukci i proti neoprávněnému přístupu).</li> <li>● Dodavatel zajistí plány obnovy po havárii technického prvku do času stanoveného Objednatelem.</li> <li>● Dodavatel umožní šifrování logických disků.</li> <li>● Dodavatel umožní šifrování databází.</li> <li>● Dodavatel zajistí dodržení standardů bezpečnosti přístupu k šifrovacím klíčům, za které odpovídá, a jejich pravidelnou obměnu.</li> <li>● Dodavatel zajistí plány obnovy systémových komponent a jejich přezkoušení nejméně 1x za rok.</li> <li>● Dodavatel zajistí sledování dostupnosti záplat instalovaných produktů a jejich řízenou instalaci.</li> <li>● Dodavatel umožní řízený upgrade SW a zařízení na vyšší verzi, na základě dohody s dodavatelem aplikací a Objednatelem.</li> </ul> <ul style="list-style-type: none"> <li>● <b>Síťová bezpečnost</b> <ul style="list-style-type: none"> <li>● Dodavatel zajistí, že prostředí aplikací Objednatele a aplikací jiných správců je odděleno firewallem případně jinými prostředky.</li> <li>● Dodavatel umožní, aby prostředí jednotlivých aplikací Objednatele bylo odděleno firewallem případně jinými prostředky.</li> <li>● Dodavatel umožní instalaci a správu firewallů (případně jiných obdobně účinných prostředků) mezi front-end (prezentační vrstvu) a back-end informačních systémů.</li> </ul> </li> </ul>
--	---

- Dodavatel zajistí firewall (případně jiný obdobně účinný prostředek) na perimetru DC.
- Dodavatel zajistí nástroj pro ochranu proti DOS a DDoS útokům na perimetru DC.
- Dodavatel zajistí vzdálený administrátorský přístup způsobem, který zajistí logování činností administrátorů.
- Dodavatel zajistí pravidelnou změnu hesel / přístupových klíčů / certifikátů a dalších využívaných autentizačních a autorizačních objektů ke konfiguraci systémových komponent.
- Dodavatel zajistí splnění požadavků na hesla v kompetenci dodavatele 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.).
- Dodavatel zajistí konfigurační standardy routerů a firewallů (případně jiných obdobně účinných prostředků).
- Dodavatel zajistí zálohování konfigurací systémových komponent při nasazování změn.
- Dodavatel zajistí implementaci anti-spoofingových opatření na perimetru DC a kontrolu jejich účinnosti nejméně 1x ročně. O zjištěných nedostatcích informuje Objednatele.
- Dodavatel zajistí aktualizaci Dokumentace skutečného provedení nejméně 1x ročně.
- Dodavatel umožní VPN přístup na úrovni operačního systému.
- Dodavatel zajistí použití šifrovacích klíčů infrastruktury Dodavatele 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.).
- Dodavatel zajistí bezpečnost přístupu k šifrovacím klíčům infrastruktury Dodavatele.
- Dodavatel umožní dvoufaktorové ověření identity pro vzdálený přístup.
- Dodavatel umožní SSL (Secure Sockets Layer) terminaci.
- Dodavatel zajistí provoz protokolů IPv4 a IPv6 ve své síti a zajistí pro ně stejnou konektivitu do externích sítí se stejnou úroveň bezpečnosti.
- Dodavatel zajistí monitoring stavu konektivity DC do/z internetu z hlediska dostupnosti a vytížení. Monitoring aktivně upozorňuje na vybočení ze stanovených limitů.
- Dodavatel 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.
- Dodavatel zajistí komunikaci s CMS, která bude zabezpečena proti odposlechu i nežádoucí modifikaci v části pod správou Dodavatele svého přístupového bodu do přístupového bodu CMS

Dodavatel se zavazuje předat informace a dokumentaci dle článků 17 a 18 Smlouvy, dodržovat principy ITIL a je povinen zajistit účast expertů na jednání, pokud si je Objednatel vyžádá.



<p>Režim služby</p>	<p>Režim 7 x 24</p> <p>Při výpadku služby je Dodavatel povinen bezodkladně informovat Objednatele o výpadku, o obnovení služby; dále je Dodavatel povinen:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> <li>- Po dobu 24 hodin denně disponovat telefonním číslem („hotline“), kde je možno oznámit případný problém, resp. zjistit stav průběhu nápravy.</li> </ul>
<p>SLA</p>	<p>Dodavatel je povinen plnit službu průběžně.</p> <p>Za každých započatých 6 hodin výpadku služby, který způsobil Dodavatel, a který způsobil bezpečnostní problém (problém bylo nutno hlásit NBÚ), se snižuje hodnota plnění za fakturační období, ve kterém byl problém zjištěn, o 10 % za KL.</p> <p>Nastane-li v měsíci více výpadků služby, postihy se v daném období sčítají, a to až do výše měsíčního plnění.</p>

## 2 Služba technického provozu a poskytování virtuální infrastruktury – KL002

Služba technického provozu a poskytování virtuální infrastruktury	
Kód služby	<b>KL002</b>
Název služby	<b>Služba technického provozu a poskytování virtuální infrastruktury</b>
Cíl služby	Cílem služby je poskytování virtuální a fyzické infrastruktury a souvisejících služeb pro provoz aplikace Objednatele v datových centrech Dodavatele.
Popis služby	<p><b><u>Společné služby</u></b></p> <p><b>Požadavky na bezpečnost:</b></p> <ul style="list-style-type: none"> <li>• Služba bude poskytována v souladu s KL001</li> </ul> <p><b>Požadavky na datová centra:</b></p> <p>Dodavatel 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.</p> <p>Produkční datová centra (DC) jsou propojena dostatečně výkonným a bezpečným datovým spojením umožňující geografické rozložení dat dopravně správních agend, resp. dalších agend Ministerstva dopravy a dále pak bezpečně propojena s datovým centrem pro umístění arbitrážního systému (komunikujícím s oběma DC).</p> <p>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 rozložení 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).</p> <p>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 Dodavatele.</p> <p>Produkční datová centra musí být připojena na Centrální místo služeb (CMS). V případě výpadku jednoho z datových center musí být provoz do CMS automaticky přesměrován do druhého datového centra Dodavatele</p> <p><b>Datová centra (produkční) musí splňovat:</b></p> <ul style="list-style-type: none"> <li>• Dostupnost DC a jeho infrastruktury minimálně 99,99%.</li> <li>• Redundance N+1 všech kritických systémů zajišťující servisovatelnost za provozu.</li> <li>• Konfigurace datových sálů v členění studená/teplá ulička nebo obdobný systém.</li> <li>• Zajištění standardních provozních teplot vhodných pro provoz informačních technologií.</li> <li>• Přesné jednotky klimatizace s nutností vzdálené správy.</li> </ul>



	<ul style="list-style-type: none"> <li>• Telekomunikační infrastruktura odpovídající úrovni požadovaných služeb.</li> <li>• Podlaha antistatická s opatřeními snižujícími prašnost.</li> <li>• Nosnost podlah DC umožňující instalovat standardní 19“ racky.</li> <li>• Monitoring a dohled celé infrastruktury 24 x 7 lokality DC.</li> </ul> <ul style="list-style-type: none"> <li>• <b>Prostředí (napájení, klimatizace)</b> <ul style="list-style-type: none"> <li>• El. energie.</li> <li>• HVAC (22±3°C, 40%-60%).</li> <li>• Detekce kouře a hašení.</li> <li>• Možnost využít samostatných prostor pro práci pracovníků Objednatele a dodavatelů přímo v lokalitě datového centra.</li> </ul> </li> <li>• <b>Konektivita</b> <ul style="list-style-type: none"> <li>• Konektivita do CMS.</li> <li>• Konektivita do internetu.</li> <li>• Dodavatel umožní realizovat požadavky na připojení jednotlivých pracovišť subjektů státní správy, samosprávy a jejich dalších datových a technologických center</li> <li>• Infrastruktura je připravena na přechod na protokol IPv6.</li> <li>• Dodavatel 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.</li> <li>• Datové linky musejí mít dostatečný přenosový výkon, a to i v případě jejich sdílení nižší přenosové vrstvy.</li> <li>• Součinnost při správě a realizaci přístupů do CMS včetně dokumentace.</li> <li>• Virtuální a fyzické servery v datových centrech Dodavatele musí mít možnost spolu komunikovat v rámci jedné sítě (L2 propojení).</li> <li>• Zajištění přístupů dle znění zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů.</li> <li>• Integrace VPN přístupů za využití VPN koncentrátoru.</li> <li>• Služba firewallů nahrazující fyzické firewally MD.</li> <li>• Služba LAN přepínačů nahrazující fyzické LAN přepínače MD.</li> <li>• Zajištění komunikace pro DSA do internetu prostřednictvím CMS dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů.</li> </ul> <p>Tato služba nebude zahrnovat poskytování a údržbu lokálních síťových infrastruktur u Objednatele – Ministerstva dopravy a přidružených OSS (Organizační složky státu).</p> </li> <li>• <b>Zajištění přístupů k datovým sítím</b> <ul style="list-style-type: none"> <li>• Dodavatel 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.</li> <li>• Dodavatel zajistí možnost vytváření privátních VLAN (Virtual Local Area Network).</li> </ul> </li> <li>• <b>Služba monitoringu</b></li> </ul>
--	---

	<p>Dodavatel poskytuje službu monitoringu jednotlivých prvků infrastruktury, za které odpovídá v následujícím rozsahu:</p> <ul style="list-style-type: none"> <li>• Provoz systému pro monitoring provozu HW, virtualizační platformy, provozovaného ostatního základního SW, servicedeskového systému.</li> <li>• 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 Dodavatele.</li> <li>• Součinnost se třetími stranami (řešení incidentů, předání informací o problémech, požadavků na změny a configuration management v rámci služeb ServiceDesku).</li> <li>• Tvorba a údržba provozní dokumentace.</li> </ul> <ul style="list-style-type: none"> <li>• <b>Služba Syslog</b> Cílem služby je poskytnout prostředí pro logování událostí infrastruktury s možností jejich zpětné analýzy v souladu s požadavky v KL001.</li> <li>• <b>Procesní provázanost služeb</b> <ul style="list-style-type: none"> <li>• Dodavatel umožní provedení změn vyplývajících z legislativních požadavků na provoz IS státní správy resp. ISO/IEC 20000 a ISO 27000</li> </ul> </li> <li>• <b>Požadovaná součinnost dodavatele</b> <ul style="list-style-type: none"> <li>• Kontinuální tvorba a údržba dokumentace prostředí.</li> <li>• Správa virtualizačního SW.</li> <li>• Návrh, posuzování, realizace a dokumentace konfiguračních změn dle požadavků Objednatele v součinnosti s 3. stranami.</li> <li>• Změny konfigurací v rozsahu běžného provozu.</li> <li>• Patchování a přechody na nové verze (nasazování nových verzí aplikací vyžadující test na speciálně vytvořeném prostředí však spadají do KL007).</li> </ul> </li> <li>• <b>Požadavky na diskovou kapacitu:</b> <ul style="list-style-type: none"> <li>• Pro aplikace tohoto katalogového listu je poskytována datová (zabezpečená) kapacita dle požadavků (s tím, že kapacita s požadavkem na georedundanci je násobena koeficientem 2,5).</li> <li>• Georedundance dat s RPO (Recovery Point Objective) blíží se hodnotě nula (0) je zajištěna pro aplikace: RSV, EUCARIS, IMIS(IFS a EGJE). Ostatní aplikace mají provozní data pouze v jedné lokalitě (záloha probíhá do druhé lokality).</li> <li>• Diskové pole musí podporovat funkcionality SnapShot.</li> <li>• Objednatel může vyžadovat až 5% kapacity na technologiích SSD. Objednatel však musí dát Dodavateli přiměřenou lhůtu k realizaci.</li> </ul> </li> </ul> <p>Požadovaný rozsah poskytované diskové kapacity(po započtení georedundance) ke dni 1.3.2019:</p>
--	--

System	min. GB
RSV	63 800
KILOMETROVNÍK	280
eTesty	6 500
IS NP	1 146
EUCARIS	1 820
IMIS, IMIS HP_UX	10 684
DSA (ADR, IS TP)	29 720
WEB MD	1 000
WEB BESIP	1 000
DK	7 001
RPSD, Ostatní	50 360
<b>Celkem</b>	<b>173 311</b>

- **Požadavky na zálohování a obnovy** (služby Managed Backup):
  - Služba zahrnuje provoz, správu a monitoring zálohovacího HW a SW Dodavatele, analýzu dat, konzultace při definici plánu zálohování.
  - 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, MS SQL, 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, RSV.
  - 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.

#### **Popis poskytování serverového výkonu HP UX**

- Servery budou umístěny v DC1 a DC2 splňující parametry uvedené výše a v KL001.

- Poskytnutí výpočetního výkonu realizovaném na technologii HP vPAR a HP Virtual Machine.
- Vyžadované prostředí pro provoz aplikací: HP UX 11i v3.
- Vyžadované prostředí pro provoz DB Oracle (verze ORA 10g, 11g).
- Servery ve virtuálním datovém centru musí spolu komunikovat v rámci datových center, v rámci jedné sítě (L2 propojení).
- Součástí služby musí být poskytnutí licencí OS HP-UX v Data Center Edici (DC-OE).

Pronájem výpočetního výkonu virtuálních serverů (HP Virtual Machine) a fyzických serverů realizovaných prostřednictvím HP vPAR pro provoz vysoce výkonných aplikačních serverů, DB serverů, provozovaných na operačním systému HP-UX 11i v3.

- Ekvivalent výkonu procesoru Itanium - jednotka vyjadřující relativní výpočetní výkon jednoho typového jádra procesoru Intel® Itanium® Processor 9540 Eight core CPU (24M Cache, 2.13 GHz).
- Typ serveru - HP Virtual Machine nebo HP vPAR.
- Množství RAM - určuje se v násobcích GB bez započtení režie virtualizace.
- Požadovaná platforma - Operační systém HP-UX 11i v3 v Datacentrové Edici.
- Požadavky na rozsah služby:
  - HP Virtual Machine (HP-UX) - v rámci služby si může Objednatel objednat libovolný virtuální server dle výkonnostního rozmezí uvedeného níže:
    - Výkon od 10% jednoho core až po 8 core procesoru Intel® Itanium® 95xx s min. frekvencí 2.13 GHz
    - Velikost RAM od 3 GB do 96 GB RAM bez započítání režie
    - HP vPAR
    - V rámci služby si může Objednatel objednat vPAR dle níže uvedených variant:
      - 2, 3, 4, 5, 6, 7, 8, 14 core procesoru Intel® Itanium® 95xx s min. frekvencí 2.13 GHz (tj. škálovatelný výkon)
    - Velikost paměti min. 8 GB RAM

Podpora a administrace až do úrovně provozu engine databáze.

#### ***Vzorová konfigurace I***

HP Integrity Blade BL860c i4 s procesory Intel® Itanium® 9540 2.13GHz/8-core/24MB/170W, nebo ekvivalent a vyšší

CPU 2x Intel® Itanium® 9540 2.13GHz (8 cores)

RAM 372 GB

NET 6x 1Gb LOM

HBA 2x FCoE FlexHBA

2x FC VC HBA

#### ***Vzorová konfigurace II***

HP Integrity Blade BL860c i4 s procesory Intel® Itanium® 9540 2.13GHz/8-core/24MB/170W, nebo ekvivalent a vyšší

CPU 2x Intel® Itanium® 9540 2.13GHz (8 cores)  
 RAM 196 GB  
 NET 6x 1Gb LOM  
 HBA 2x FCoE FlexHBA  
 2x FC VC HBA  
 HDD

### Služba poskytování virtuální infrastruktury X86/X64

Služby zahrnuje:

- Alokaci a správu virtuálního výkonu.
- Virtualizaci na platformě VMWare.
- Servery budou umístěny v DC1, DC2 splňující parametry uvedené výše a v KL001.
- Požadovaná platforma - Intel x86/x64 kompatibilní.
- Vyžadované prostředí pro provoz aplikací: OS MS Windows 2003, Windows 2008 R2, Windows 2012, CentOS, OS RedHat Linux rel 5, 6 a 7, SUSE Linux dle aktuální konfigurace případně vyšší.
- Vyžadované prostředí pro provoz DB MS SQL (2008R2, 2012): OS Windows 2008 R2, Windows 2012 dle aktuální konfigurace případně vyšší.
- Dodavatel umožní v dohodnutých případech administraci OS Objednatelem.
- Přípustný agregační poměr na virtualizační platformě je 3:1 (tedy 3vCPU na jedno fyzické jádro).
- Virtualizační řešení musí umožnit, aby Objednatel mohl využívat licence Microsoft, které již vlastní nebo je pořídí na základě vlastní smlouvy se společností Microsoft.
- Řešení musí podporovat MSCS clustery (OS Windows 2008 R2, Windows 2012) a RedHat Linux clustery.
- Podpora a administrace až do úrovně provozu engine databáze, není-li dohodnuto jinak.

### Vzorová 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  
 HDD No internal storage  
 HW Management ILO

Servery:

Agenda	VM	vCPU	vRAM [MB]	CPU	RAM	Stav	TYP
ADR		4	16 384			aktivní	virtuál
ADR		2	4 096			aktivní	virtuál
ADR		2	4 096			aktivní	virtuál

Příloha č. 1

ADR		1	4 096			aktivní	virtuál
DSA		1	2 048			aktivní	virtuál
DSA		1	2 048			aktivní	virtuál
DSA		2	4 096			aktivní	virtuál
DK		4	12 168			aktivní	virtuál
DK		4	12 168			aktivní	virtuál
DK		4	12 168			aktivní	virtuál
DK		12	65 536			aktivní	virtuál
DK		12	65 536			aktivní	virtuál
DK		6	65 536			aktivní	virtuál
DT		2	8 192			aktivní	virtuál
DT		2	8 192			aktivní	virtuál
DT		4	16 384			aktivní	virtuál
DT		4	16 384			aktivní	virtuál
DT		2	8 192			aktivní	virtuál
DT		2	8 192			aktivní	virtuál
DT		2	16 384			aktivní	virtuál
DT		2	16 384			aktivní	virtuál
eTESTY		1	4 096			aktivní	virtuál
eTESTY		1	4 096			aktivní	virtuál
eTESTY		4	16 384			aktivní	virtuál
eTESTY		4	16 384			aktivní	virtuál
eTESTY		4	16 384			aktivní	virtuál
eTESTY		4	16 384			aktivní	virtuál
eTESTY		4	16 384			aktivní	virtuál
eTESTY		4	16 384			aktivní	virtuál
eTESTY		4	16 384			aktivní	virtuál
eTESTY		8	32 768			aktivní	virtuál
eTESTY		8	32 768			aktivní	virtuál
eTESTY		1	4 096			aktivní	virtuál
eTESTY		2	8 192			aktivní	virtuál
eTESTY		2	16 384			aktivní	virtuál
IMIS		2	4 096			aktivní	virtuál
IMIS		2	4 096			aktivní	virtuál
IMIS		2	4 096			aktivní	virtuál
IMIS		2	4 096			aktivní	virtuál
IMIS		2	3 072			aktivní	virtuál
IMIS		2	3 072			aktivní	virtuál
IMIS		2	4 096			aktivní	virtuál
IMIS		4	12 228			aktivní	virtuál

Příloha č. 1

IMIS		4	12 228			aktivní	virtuál
IMIS		4	12 228			aktivní	virtuál
IMIS		4	12 228			aktivní	virtuál
IMIS		4	12 228			aktivní	virtuál
IMIS		4	12 228			aktivní	virtuál
IMIS		4	8 192			aktivní	virtuál
IMIS		4	4 096			aktivní	virtuál
IMIS		4	4 096			aktivní	virtuál
IMIS		4	4 096			aktivní	virtuál
IMIS		1	512			aktivní	virtuál
IMIS			4		32 768	aktivní	fyzický
IMIS			4		32 768	aktivní	fyzický
IMIS			1		16 384	aktivní	fyzický
IMIS		4	16 384			aktivní	virtuál
IMIS		2	8 192			aktivní	virtuál
IMIS		1	512			aktivní	virtuál
INFRA		2	4 096			aktivní	virtuál
INFRA		1	2 048			aktivní	virtuál
INFRA		1	2 048			aktivní	virtuál
INFRA		2	4 096			aktivní	virtuál
INFRA		1	2 048			aktivní	virtuál
INFRA		4	8 192			aktivní	virtuál
INFRA		2	2 048			aktivní	virtuál
INFRA		4	16 384			aktivní	virtuál
INFRA		4	16 384			aktivní	virtuál
INFRA		4	16 384			aktivní	virtuál
INFRA		1	2 048			aktivní	virtuál
INFRA		4	4 096			aktivní	virtuál
INFRA						zrušeno	virtuál
INFRA						zrušeno	virtuál
INFRA						zrušeno	virtuál
INFRA		10	24 576			aktivní	virtuál
INFRA		10	16 384			aktivní	virtuál
IS NP		1	4 096			aktivní	virtuál
IS NP		1	4 096			aktivní	virtuál
IS NP		4	8 192			aktivní	virtuál
IS NP		4	8 192			aktivní	virtuál
IS NP		2	8 192			aktivní	virtuál

Příloha č. 1

	IS NP		2	8 192			aktivní	virtuál
	IS NP		4	12 288			aktivní	virtuál
	IS NP		4	12 288			aktivní	virtuál
	IS NP		1	4 096			aktivní	virtuál
	IS NP		1	4 096			aktivní	virtuál
	IS NP		4	8 192			aktivní	virtuál
	IS NP		4	8 192			aktivní	virtuál
	IS NP		2	8 192			aktivní	virtuál
	IS NP		2	8 192			aktivní	virtuál
	IS NP		4	12 288			aktivní	virtuál
	IS NP		4	12 288			aktivní	virtuál
	NKM/EUCARIS		2	8 192			aktivní	virtuál
	NKM/EUCARIS		2	8 192			aktivní	virtuál
	NKM/EUCARIS		4	16 384			aktivní	virtuál
	NKM/EUCARIS		4	16 384			aktivní	virtuál
	NKM/EUCARIS		2	8 192			aktivní	virtuál
	NKM/EUCARIS		2	8 192			aktivní	virtuál
	NKM/EUCARIS		4	8 192			aktivní	virtuál
	NKM/EUCARIS		4	10 240			aktivní	virtuál
	NKM/EUCARIS		4	10 240			aktivní	virtuál
	NKM/EUCARIS		2	10 240			aktivní	virtuál
	NKM/EUCARIS		2	10 240			aktivní	virtuál
	NKM/EUCARIS		4	24 576			aktivní	virtuál
	NKM/EUCARIS		4	24 576			aktivní	virtuál
	RPSD		2	4 096			aktivní	virtuál
	RPSD		6	24 576			aktivní	virtuál
	RPSD		6	24 576			aktivní	virtuál
	RPSD		8	65 536			aktivní	virtuál
	RPSD		8	65 536			aktivní	virtuál
	RPSD		4	16 384			aktivní	virtuál
	RPSD		4	32 768			aktivní	virtuál
	RSV		2	4 096			aktivní	virtuál
	RSV		2	4 096			aktivní	virtuál
	RSV		4	8 192			aktivní	virtuál



Příloha č. 1

RSV	4	8 192			aktivní	virtuál
RSV	4	12 288			aktivní	virtuál
RSV	4	12 288			aktivní	virtuál
RSV	4	12 288			aktivní	virtuál
RSV	4	12 288			aktivní	virtuál
RSV	4	12 288			aktivní	virtuál
RSV	4	12 288			aktivní	virtuál
RSV	4	12 288			aktivní	virtuál
RSV	4	12 288			aktivní	virtuál
RSV	4	8 192			aktivní	virtuál
RSV	2	4 096			aktivní	virtuál
RSV	2	4 096			aktivní	virtuál
RSV	4	8 192			aktivní	virtuál
RSV	6	49 152			aktivní	virtuál
RSV	4	8 192			aktivní	virtuál
RSV	4	8 192			aktivní	virtuál
RSV			-	-	zrušeno	virtuál
RSV			-	-	zrušeno	virtuál
RSV	16			512 000	aktivní	fyzický
RSV	16			512 000	aktivní	fyzický
IS TP	2	4 096			aktivní	virtuál
IS TP	2	4 096			aktivní	virtuál
IS TP	2	4 096			aktivní	virtuál
IS TP	2	4 096			aktivní	virtuál
IS TP	6	65 536			aktivní	virtuál
IS TP	6	65 536			aktivní	virtuál
IS TP	2	32 768			aktivní	virtuál
IS TP	2	32 768			aktivní	virtuál
IS TP	4	12 288			aktivní	virtuál
IS TP	4	12 288			aktivní	virtuál
KILOMETROVNÍK	4	6 144			aktivní	virtuál
STK/KILOMETROVNÍK			-	-	zrušeno	virtuál
KILOMETROVNÍK	4	8 192			aktivní	virtuál
WEB/BESIP	2	12 288			aktivní	virtuál
WEB/BESIP	2	12 288			aktivní	virtuál

## Příloha č. 1

WEB/BESIP		4	24 576			aktivní	virtuál
WEB/BESIP		2	12 288			aktivní	virtuál
WEB/BESIP		4	24 576			aktivní	virtuál

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.

Objednatel může požadovat také ročně nárůst kapacity diskových polí až do výše 10% bez navýšení ceny. Na nárůst kapacity jsou navázány i příslušné služby záloh bez vlivu na cenu.

Počáteční objem pro výpočet navýšení je 120 000 GB diskové kapacity, 414 vCPU, 1397 GB RAM.

Možné navýšení zdrojů pro prvních 5 let je tedy:

	Disková kapacita (GB)	vCPU (ks)	RAM (MB)
<b>Počáteční stav</b>	120 000	414	1 397
<b>25.9.2018</b>	132 000	455	1 537
<b>25.9.2019</b>	145 000	501	1 690
<b>25.9.2020</b>	160 000	551	1 859
<b>25.9.2021</b>	176 000	606	2 045
<b>25.9.2022</b>	194 000	667	2 250

### Služba fyzických serverů

Zahrnuje poskytování dedikovaného fyzického DB Geoclusteru vč – licencí pro agendy RSV PROD a EUCARIS PROD

Parametry fyzických serverů:

Server	vCPU	RAM	Licence zajišťuje	Licenční program	OS licence	DB licence
	16	512	O2 ITS	SPLA	OS WIN 2016	MS SQL 2016 Ent.
	16	512	O2 ITS	SPLA	OS WIN 2016	MS SQL 2016 Ent.

### Služba Licencování

Pro podporu jednotlivých agend je využívána zejména služba licencování, tj. poskytnutí licencí formou SPLA. Stav požadovaný k 1. 8. 2018:

Příloha č. 1

VM	Agenda	Licence zajišťuje	Licenční program	OS licence	SW Licence
	ADR	MD	ve vlastnictví MD	OS Win Ser 2008R2	DB MS SQL 2008 Std.
	ADR	MD	ve vlastnictví MD	OS Win Ser 2008R2	DB MS SQL 2008 Std.
	ADR	MD	ve vlastnictví MD	OS Win Ser 2008R2	
	ADR	MD	ve vlastnictví MD	OS Win Ser 2008R2	
	DSA	MD	ve vlastnictví MD	OS Win Ser 2008R2	
	DSA	MD	ve vlastnictví MD	OS Win Ser 2008R2	
	DSA	MD	ve vlastnictví MD	OS Win Ser 2008R2	DB MS SQL 2008 Std.
	DK	O2 ITS	SPLA	OS WIN 2016 Std.	
	DK	O2 ITS	SPLA	OS WIN 2016 Std.	
	DK	O2 ITS	SPLA	OS WIN 2016 Std.	
	DK	O2 ITS	SPLA	OS WIN 2016 Std.	MS SQL Standard (KMSTK - 2012) (DK - 2016)
	DK	O2 ITS	SPLA	OS WIN 2016 Std.	
	DK	O2 ITS	SPLA	OS WIN 2016 Std.	
	DT	O2 ITS	SPLA	OS WIN 2016 Std.	
	DT	O2 ITS	SPLA	OS WIN 2016 Std.	
	DT	O2 ITS	SPLA	OS WIN 2016 Std.	DB MS SQL 2016 Std.
	DT	O2 ITS	SPLA	OS WIN 2016 Std.	
	DT	O2 ITS	SPLA	OS WIN 2016 Std.	
	DT	O2 ITS	SPLA	OS WIN 2016 Std.	DB MS SQL 2016 Std.
	DT	O2 ITS	SPLA	OS WIN 2016 Std.	
	eTESTY <sup>2)</sup>	MD	ve vlastnictví MD	OS Win Ser 2012, External Connector	
	eTESTY <sup>2)</sup>	MD	ve vlastnictví MD	OS Win Ser 2012, External Connector	
	eTESTY <sup>2)</sup>	MD	ve vlastnictví MD	OS Win Ser 2012, External Connector	
	eTESTY <sup>2)</sup>	MD	ve vlastnictví MD	OS Win Ser 2012, External Connector	

Příloha č. 1

	eTESTY <sup>2)</sup>	MD	ve vlastnictví MD	OS Win Ser 2012, External Connector	
	eTESTY <sup>2)</sup>	MD	ve vlastnictví MD	OS Win Ser 2012, External Connector	
	eTESTY <sup>2)</sup>	MD	ve vlastnictví MD	OS Win Ser 2012, External Connector	
	eTESTY <sup>2)</sup>	MD	ve vlastnictví MD	OS Win Ser 2012, External Connector	
	eTESTY <sup>2)</sup>	MD	ve vlastnictví MD	OS Win Ser 2012, External Connector	DB MS SQL 2012 Std.
	eTESTY <sup>2)</sup>	MD	ve vlastnictví MD	OS Win Ser 2012, External Connector	DB MS SQL 2012 Std.
	eTESTY	O2 ITS	SPLA	OS Win Ser 2012	
	eTESTY	O2 ITS	SPLA	OS Win Ser 2012	
	eTESTY	O2 ITS	SPLA	OS Win Ser 2012	DB MS SQL 2012 Std.
	EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	
	EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	
	EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	
	IMIS	MD	SPLA	OS Win Ser 2008R2	Citrix
	IMIS	MD	SPLA	OS Win Ser 2008R2	Citrix
	IMIS	MD	ve vlastnictví MD	SUSE Linux Enterprise 11 (64-bit)	RSA appliance
	IMIS	MD	ve vlastnictví MD	SUSE Linux Enterprise 11 (64-bit)	RSA appliance
	IMIS	MD	ve vlastnictví MD	OS Win Ser 2003	
	IMIS	MD	ve vlastnictví MD	OS Win Ser 2003	
	IMIS	O2 ITS	SPLA	OS Win Ser 2008R2	Citrix
	IMIS	O2 ITS	SPLA	OS Win Ser 2008R2	Citrix
	IMIS	O2 ITS	SPLA	OS Win Ser 2008R2	Citrix
	IMIS	O2 ITS	SPLA	OS Win Ser 2008R2	Citrix
	IMIS	O2 ITS	SPLA	OS Win Ser 2008R2	Citrix
	IMIS	O2 ITS	SPLA	OS Win Ser 2008R2	Citrix
	IMIS	O2 ITS	SPLA	OS Win Ser 2008R2	Citrix
	IMIS	O2 ITS	SPLA	OS Win Ser 2008R2	Citrix
	IMIS	O2 ITS	SPLA	OS Win Ser 2008R2	Citrix
	IMIS	MD	ve vlastnictví MD	OS Win Ser 2003	Citrix
	IMIS	MD	SPLA	OS Win Ser 2008R2	Citrix
	IMIS	MD	SPLA	OS Win Ser 2008R2	Citrix

Příloha č. 1

		IMIS	MD	ve vlastnictví MD	CentOS (64-bit)	
		IMIS	MD (DB lic)	ve vlastnictví MD	OS HP-UX 11i - poskytován jako služba O2ITS,	Oracle DB
		IMIS	MD (DB lic)	ve vlastnictví MD	OS HP-UX 11i - poskytován jako služba O2ITS,	Oracle DB
		IMIS	MD (DB lic)	ve vlastnictví MD	OS HP-UX 11i - poskytován jako služba O2ITS,	Oracle DB
		IMIS	O2 ITS	SPLA	OS Win Ser 2012	
		IMIS	O2 ITS	SPLA	OS Win Ser 2012	
		IMIS	MD	ve vlastnictví MD	CentOS (64-bit)	
		INFRA	MD	ve vlastnictví MD	OS Win Ser 2008R2	
		INFRA	MD	ve vlastnictví MD	OS Win Ser 2008R2	
		INFRA	MD	ve vlastnictví MD	OS Win Ser 2008R2	
		INFRA	MD	ve vlastnictví MD	OS Win Ser 2008R2	
		INFRA	MD	ve vlastnictví MD	OS Win Ser 2008R2	
		INFRA	MD	ve vlastnictví MD	SUSE Linux Enterprise 11 (64-bit)	-
		INFRA	MD	ve vlastnictví MD	OS Win Ser 2008R2	-
		INFRA	MD	ve vlastnictví MD	OS Win Ser 2008R2	-
		Infra O2/Backup	O2 ITS	SPLA	OS Win Ser 2012	
		Infra O2/Backup	O2 ITS	SPLA	OS Win Ser 2012	
		Infra O2/Monitoring	O2 ITS	vlastnictví O2ITS	CentOS 4/5/6 (32-bit)	
		Infra O2/Monitoring	O2 ITS	vlastnictví O2ITS	CentOS 4/5/6 (32-bit)	
		Infra O2/SEC	O2 ITS	vlastnictví O2ITS	CentOS 4/5/6/7 (64-bit)	
		Infra O2/SEC	O2 ITS	vlastnictví O2ITS	CentOS 4/5/6/7 (64-bit)	
		Infra O2/SEC	O2 ITS	vlastnictví O2ITS	CentOS 4/5/6/7 (64-bit)	
		Infra O2/SEC	O2 ITS	vlastnictví O2ITS	CentOS 4/5/6/7 (64-bit)	
		Infra O2/SEC	O2 ITS	SPLA	OS WIN 2016 Std.	
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	

Příloha č. 1

		IS NP	O2 ITS	SPLA	OS Win Ser 2012	
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	DB MS SQL 2012 Std.
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	DB MS SQL 2012 Std.
		IS NP	O2 ITS	SPLA	OS Win Ser 2012	
		NKM/EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	
		NKM/EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	
		NKM/EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	DB MS SQL 2016 Std.
		NKM/EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	
		NKM/EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	
		NKM/EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	
		NKM/EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	
		NKM/EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	
		NKM/EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	
		NKM/EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	DB MS SQL 2016 Std.*
		NKM/EUCARIS	O2 ITS	SPLA	OS WIN 2016 Std.	
		RPSD	MD	ve vlastnictví MD	CentOS 4/5/6/7 (64-bit)	
		RPSD	MD	ve vlastnictví MD	Red Hat Enterprise Linux 6 (64-bit)	
		RPSD	MD	ve vlastnictví MD	Red Hat Enterprise Linux 6 (64-bit)	
		RPSD	MD	ve vlastnictví MD	Red Hat Enterprise Linux 6 (64-bit)	
		RPSD	MD	ve vlastnictví MD	Red Hat Enterprise Linux 6 (64-bit)	



	IS TP	O2 ITS	SPLA	OS Win Ser 2008R4	DB MS SQL 2008 Std.
	IS TP	O2 ITS	SPLA	OS Win Ser 2008R5	DB MS SQL 2008 Std.
	Kilometrovník	O2 ITS	SPLA	OS Win Ser 2012	
	STK/Kilometrovník	O2 ITS	SPLA	OS Win Ser 2012	DB MS SQL 2012 Std.
	Kilometrovník	O2 ITS	SPLA	OS Win Ser 2012	DB MS SQL 2012 Std.
	WEB	O2 ITS	SPLA	OS Win Ser 2012	
	WEB/Besip	O2 ITS	SPLA	OS Win Ser 2012	
	WEB/Besip	O2 ITS	SPLA	OS Win Ser 2012	DB MS SQL 2012 Web edice*
	WEB/Besip	O2 ITS	SPLA	OS Win Ser 2012	
	WEB/Besip	O2 ITS	SPLA	OS Win Ser 2012	DB MS SQL 2012 Web edice*

V rámci programu poskytování licencí SPLA jsou u agendy využívány verze OS a DB dle potřeb aplikací.

\* Prostředí vč. Licencí je sdíleno dvěma agendami

<sup>2)</sup> eTESTY byly zprovozněny na základě vlastněných licencí Ministerstvem dopravy, a to:

- Microsoft SQL Std Core 2014 v počtu 8 ks, instalována verze 2012 (downgrade)
- Microsoft SQL Std Core 2016 v počtu 8 ks, instalována verze 2012 (downgrade)
- Microsoft Server 2012 R2 2proc v počtu 5 ks
- Microsoft Server 2012 External Connector v počtu 5 ks

Verze použitých prostředí mohou být ke dni převzetí provozu Dodavatelem změněny na základě pravidelných upgrade, resp. na základě potřeb vyvolaných upgrade aplikací provedených v období od podpisu Smlouvy do převzetí podpory dané oblasti Dodavatelem.

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

### **Služba provozu aplikací RSV a EUCARIS**

Prostředí a služby:

- Fyzický databázový geocluster (platforma X86/x64)
- Virtuální georedundantní prostředí pro aplikace (platforma X86/x64)
- On-line replikace dat mezi DC (RPO blíží se nule)
- Podpora OS a engine DB
- Zálohování
- Dokumentace infrastrukturního prostředí
- Konektivita
- Dohledy



- Vystavení aplikace RSV do produkce, nasazení aplikace EUCARIS a NKM zajišťuje aplikační dodavatel a je zodpovědný za provoz.

### **Služba provozu aplikací ERP, HR (IMIS)**

#### Prostředí a služby:

- Databázový geocluster ORACLE (platforma HP-UX)
- Virtuální georedundantní prostředí pro aplikaci (platforma X86/x64)
- On-line replikace dat mezi DC prostřednictvím ORACLE RAC (RPO blíží se nule)
- Podpora OS a engine DB
- Zálohování
- Dokumentace infrastrukturního prostředí
- Konektivita
- Dohledy
- Vystavení aplikace do produkce

### **Služba provozu aplikace eTesty, DT a IS NP**

#### Prostředí a služby:

- Virtuální georedundantní prostředí pro aplikace (platforma X86/x64)
- Podpora OS a engine DB
- Zálohování
- Dokumentace infrastrukturního prostředí
- Konektivita
- Dohledy
- Vystavení aplikace do produkce

### **Služba provoz aplikace IS TP, Kilometrovník, ADR, WEBy**

#### Prostředí a služby:

- Virtuální prostředí pro aplikace (platforma X86/x64)
- Podpora OS a engine DB
- Zálohování
- Dokumentace infrastrukturního prostředí
- Konektivita
- Dohledy
- Vystavení aplikace do produkce

### **Služba provoz aplikace RPSD**

#### Prostředí a služby:

- Virtuální prostředí pro aplikace (platforma X86/x64)
- Zálohování s využitím agenta 3. strany
- Dokumentace infrastrukturního prostředí
- Konektivita
- Dohledy virtuální platformy

	<p>Dodavatel se zavazuje předat informace a dokumentaci dle článků 17 a 18 Smlouvy, dodržovat principy ITIL a je povinen zajistit účast expertů na jednání s dodavatelem 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.</p> <p>Objednatel může čerpat nevyužitou kapacitní a výkonovou 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.</p>		
<b>SLA parametry dostupnosti služby</b>			
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
Služba provozu OS a DB aplikací RSV a EUCARIS – 7x24	99,00	24 x 7	120
Služby potřebné k provozování OS, DB, úložiště dat, zálohování a komunikační infrastruktury aplikací ERP, HR	98,00	5 x 10 (Po-Pa, 8:00 – 18:00)	120
Služby potřebné k provozování OS, DB, úložiště dat, zálohování a komunikační infrastruktury ostatních aplikací	98,00	24 x 7	120
<b>SLA parametry řešení incidentů</b>			
<p>Při výpadku služby je Dodavatel povinen bezodkladně informovat Objednatele o výpadku, o obnovení služby; dále je Dodavatel povinen:</p> <ul style="list-style-type: none"> <li>- 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.</li> </ul>			

**Příloha č. 1**

- 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 přijetí Incidentu / Servisního požadavku do doby vyřešení Incidentu / Servisního požadavku. Do Doby vyřešení není započítáván čas čekání na součinnost Objednatele nebo dodavatele 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	Služba nebo její část je celkově nedostupná a nedostupností jsou postiženi všichni uživatelé dané služby nebo významná skupina uživatelů (ORP, MD, Celní správa, ČKP, exekutoři, Policie ČR a další složky s oprávněným přístupem k údajům aplikací). 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	Služba nebo její část je mírně omezená a touto mírnou omezeností jsou postiženi všichni uživatelé dané služby nebo významná skupina uživatelů. Incident omezuje uživatele, avšak nedochází k ohrožení termínu nebo existuje známé náhradní řešení.		
	Priorita 3	Ostatní incidenty.		
Plánované odstávky				
každou středu 22:00 – 5:00, maximálně na dobu 5 hodin nebo dle dohody s Objednatelem				
<b>Vymezující podmínky</b>				
Skupina uživatelů				
pracovníci Ministerstva dopravy (MD) pracovníci OSS pracovníci obcí s rozšířenou působností (ORP) Policie ČR				

<p>Celní správa ČKP Exekutoři, komisaři další složky s oprávněným přístupem</p>
<p>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 Dodavatele Objednatele.</p>
<p><b>Měření dostupnosti</b></p>
<p>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 Dodavatel, 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 %.</p> <p style="text-align: center;"><b>Dostupnost</b> = <math>(PD_{\text{období}} - N_{\text{služby}}) / PD_{\text{období}} * 100</math> [%]</p> <p>Kde:</p> <p style="padding-left: 40px;"><math>PD_{\text{období}}</math> .... Odsouhlasená provozní doba za sledované období</p> <p style="padding-left: 40px;"><math>N_{\text{služby}}</math> ..... Doba úplné nedostupnosti služby ve sledovaném období, za níž odpovídá Dodavatel</p> <p>Pro určení slevy za nedodržení dostupnosti je rozhodující jak „Maximální doba jednoho výpadku služby“, tak „Dostupnost služby měsíční“.</p> <p>Za každé překročení maximální doby jednoho výpadku služby je poskytnuta sleva v souladu se smlouvou v příslušné prioritě.</p> <p>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.</p> <p>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.</p>
<p><b>Měření doby vyřešení</b></p>
<p>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.</p> <p>Doba vyřešení v %:</p> <p style="text-align: center;"><b>Doba vyřešení</b> = <math>(PI - PNI) / PI * 100</math> [%]</p>

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

Pro určení slevy za nedodržení doby vyřešení je rozhodující „Plnění v %“.

Pokud je skutečné plnění větší nebo rovno než uvedená hodnota ve sloupci „Plnění v %“, sleva na jednotlivé překročení doby vyřešení se neuplatňuje.

Pokud je skutečné plnění menší než uvedená hodnota ve sloupci „Plnění v %“, sleva se uplatňuje, a to pro každé jednotlivé překročení doby vyřešení, tj. slevy se sčítají. Výše slevy je dána Smlouvou s ohledem na prioritu nahlášeného incidentu (servisního požadavku).

Měření a výpočet doby vyřešení se provádí za každou prioritu samostatně. Pokud je nárok na slevy za více priorit, tyto slevy se sčítají.

### 3 Služba provozu CRŘ – KL003

Kód služby	<b>KL003</b>
Název služby	<b>Služba provozu prostředí CRŘ</b>
Cíl služby	Cílem služby je poskytovat prostředí pro provoz HW a SW provozovatele Centrálního registru řidičů (CRŘ)
Popis služby	<p>Plnění služby musí být v souladu s KL001. Provoz bude zajištěn v DC s parametry dle KL002.</p> <p>Pro provozovatele aplikace je zapotřebí zajistit prostředí, které provozovateli aplikace umožní umístění:</p> <ul style="list-style-type: none"> <li>• 2 x skříň 42U, 2x nezávislé napájení 400V/16A zajištěné proti výpadku, který bude obsahovat systémy dodané provozovatelem aplikace. Do skříní je aktuálně umístěno: <ul style="list-style-type: none"> <li>○ 25 serverů</li> <li>○ Disková pole o datové kapacitě 5 TB (z toho 3TB v RAID10)</li> <li>○ Ovládací konzole, KVM přepínač</li> </ul> </li> <li>• Skříň bude možné zamknout či plombovat</li> <li>• Příkon odpovídající jističům min. 3*32A a 3*16A a odpovídající chlazení</li> </ul> <p>Dále je pro tyto systémy požadováno:</p> <ul style="list-style-type: none"> <li>• 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, CRŘ.</li> <li>• 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 Objednatel pro aplikaci CRŘ. Nektivita s CMS min. 20Mb/s (redundantní)</li> <li>• VPN management připojení pro 4 administrátory linkou min. 5Mbit/s z internetu</li> <li>• 24x7 fyzický přístup pro 4 administrátory do DC a dohled obsluhy DC</li> <li>• Možnost konektivity (publikace) i přes internet</li> <li>• Návrh, posuzování, realizace a dokumentace konfiguračních změn dle požadavků Objednatel v součinnosti s 3. stranami</li> <li>• Změny konfigurací systémů zajišťovaných v rámci tohoto KL</li> <li>• Přechody na nové verze systémů zajišťovaných v rámci tohoto KL (nasazování nových verzí aplikací vyžadující test na speciálně vytvořeném prostředí však spadají do KL007)</li> </ul> <p>Dodavatel se zavazuje předat informace a dokumentaci dle článků 17 a 18 Smlouvy, dodržovat principy ITIL a je povinen zajistit účast expertů na jednání</p>

	s dodavatelem podpory a rozvoje aplikace alespoň jedenkrát za týden (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.			
	Zálohy se v případě provozu aplikace jen v jednom datovém centru vždy ukládají v geograficky vzdáleném datovém centru s úrovní Tier 3.			
<b>SLA parametry dostupnosti služby</b>				
Při výpadku služby je Dodavatel povinen bezodkladně informovat Objednatele o výpadku, o obnovení služby; dále je Dodavatele povinen:				
<ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> </ul>				
Služba	Dostupnost služby měsíční (v %)	Rozsah zaručeného provozu služby	Max.doba jednoho výpadku služby (v minutách)	
Služby Datového centra	99,99	24 x 7	30	
Další služby KL	98,00	24 x 7	120	
<b>SLA parametry řešení incidentů</b>				
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 dodavatele 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	Služba nebo její část je celkově nedostupná a nedostupností jsou postiženi všichni uživatelé dané služby nebo významná skupina uživatelů (ORP, MD, Celní správa, Policie ČR a další složky s oprávněným přístupem k údajům CRR). 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	Služba nebo její část je mírně omezená a touto mírnou omezeností jsou postiženi všichni uživatelé dané služby nebo významná skupina uživatelů. Incident omezuje uživatele, avšak nedochází k ohrožení termínu nebo existuje známé náhradní řešení.
	Priorita 3	Ostatní incidenty
Plánované odstávky		
každou středu 22:00 – 5:00, maximálně na dobu 5 hodin nebo dle dohody s Objednatelem		
<b>Vymezující podmínky</b>		
Skupina uživatelů		
Policie ČR Obce s rozšířenou působností pracovníci Ministerstva dopravy (MD) další složky s oprávněným přístupem		
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 Dodavatele Objednatele.		
<b>Měření dostupnosti</b>		
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 Dodavatel, 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 %.		
<b>Dostupnost</b> = $(PD_{\text{období}} - N_{\text{služby}}) / PD_{\text{období}} * 100$ [%]		
Kde:		
PD <sub>období</sub> .... Odsouhlasená provozní doba za sledované období		
N <sub>služby</sub> ..... Doba úplné nedostupnosti služby ve sledovaném období, za níž odpovídá Dodavatel		
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.

Doba vyřešení v %:

$$\text{Doba vyřešení} = (PI - PNI) / PI * 100 \text{ [\%]}$$

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

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

Pro určení slevy za nedodržení doby vyřešení je rozhodující „Plnění v %“.

Pokud je skutečné plnění větší nebo rovno než uvedená hodnota ve sloupci „Plnění v %“, sleva na jednotlivé překročení doby vyřešení se neuplatňuje.

Pokud je skutečné plnění menší než uvedená hodnota ve sloupci „Plnění v %“, sleva se uplatňuje, a to pro každé jednotlivé překročení doby vyřešení, tj. slevy se sčítají. Výše slevy je dána Smlouvou s ohledem na prioritu nahlášeného incidentu (servisního požadavku).

Měření a výpočet doby vyřešení se provádí za každou prioritu samostatně. Pokud je nárok na slevy za více priorit, tyto slevy se sčítají.

#### 4 Služba provozu Call Centra– KL004

Kód služby	<b>KL004</b>
Název služby	<b>Služba provozu Call Centra</b>
Cíl služby	Cílem služby je zajistit jednotný systém správy požadavků, incidentů, problémů a změn a jejich monitoring, vyhodnocování a reporting
Popis služby	<p>Service Desk</p> <p>V rámci této služby budou poskytovány činnosti související s provozem jednoho kontaktního místa (single point of contact-SPOC) pro uživatele služeb aplikačního provozu (ERP, HR, IS NP, IS TP) 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 a emailové adrese a bude zajištěno operátorským zabezpečením ze strany Dodavatele.</p> <p>Na definovanou Zelenou linku a emailovou adresu budou hlášeny veškeré incidenty, požadavky a problémy uživatelů aplikačního provozu ERP, HR, IS NP, IS TP a kontaktních osob pro služby virtuální infrastruktury.</p> <p>V případě nejasností se stanovením priority incidentu je Dodavatel povinen konzultovat s Objednatelem (zadavatelem incidentu) správnou hodnotu priority. V případě nesouladu stanovení priority Dodavatelem s KL má Objednatel právo požadovat správné nastavení priority. Dodavatel je pak povinen s touto prioritou pracovat tak, jako by byla nastavena od samého počátku.</p> <p>Služba Service desk bude zajišťovat a podporovat následující činnosti:</p> <p>pro ERP, HR a IS NP:</p> <ul style="list-style-type: none"> <li>• řízení životního cyklu Incidentu</li> <li>• řízení životního cyklu Požadavku</li> <li>• řízení životního cyklu Požadavku na změnu</li> <li>• komunikace s Objednatelem</li> <li>• reporting</li> <li>• součinnost se 3. stranami</li> <li>• tvorba a údržba provozní dokumentace týkající se služby Service Desk</li> </ul> <p>pro RSV a IS TP:</p> <ul style="list-style-type: none"> <li>• příjem, evidence a zaslání řešiteli nahlášených Incidentů</li> <li>• příjem, evidence a zaslání řešiteli nahlášených Požadavků</li> <li>• příjem, evidence a zaslání řešiteli nahlášených Požadavků na změnu</li> <li>• reporting</li> <li>• součinnost se 3. stranami</li> </ul>

	<p>Řízení životního cyklu Incidentu</p> <ul style="list-style-type: none"> <li>• plnění role 1. úrovně podpory v procesu Incident Managementu, kam především patří: <ul style="list-style-type: none"> <li>○ příjem Incidentů</li> <li>○ analýza Incidentů</li> <li>○ kategorizace Incidentů</li> <li>○ prvotní řešení incidentů, je-li k dispozici databáze známých chyb</li> <li>○ předávání řešení incidentů na 2. úroveň podpory (dle metodiky ITIL)</li> <li>○ sledování a průběžná kontrola řešení Incidentů</li> <li>○ ověřování vhodnosti řešení u uživatele</li> <li>○ uzavírání Incidentů</li> </ul> </li> <li>• Koordinace 2. a 3. úrovně podpory v procesu Incident Managementu (dle metodiky ITIL)</li> <li>• Zajišťování funkční či hierarchické eskalace</li> </ul> <p>Řízení životního cyklu Požadavku</p> <ul style="list-style-type: none"> <li>• identifikace požadavku</li> <li>• předání požadavku na řešitele</li> <li>• sledování a průběžná kontrola řešení požadavku</li> <li>• ověřování řešení u uživatele</li> <li>• uzavírání požadavku</li> </ul> <p>Řízení životního cyklu Požadavku na změnu</p> <ul style="list-style-type: none"> <li>• příjem a evidence Požadavku na změnu</li> <li>• předávání Požadavků na změnu na vyjádření Metodickému oddělení Objednatele</li> <li>• předávání Požadavků na změnu k realizaci dodavatelům</li> <li>• sledování a průběžná kontrola plnění Požadavků na změnu</li> </ul> <p>Komunikace s Objednatelem</p> <ul style="list-style-type: none"> <li>• průběžná informovanost Objednatele o stavu vyřizování jimi hlášených incidentů, problémů a požadavků</li> <li>• informování Objednatele a jeho uživatelů o plánovaných odstávkách systémů, o připravovaných změnách a dopadu těchto změn a odstávek.</li> <li>• generování automatických hlášení prostřednictvím elektronické pošty na definované pracoviště Objednatele</li> </ul> <p>Reporting</p> <ul style="list-style-type: none"> <li>• Příprava standardních a zákaznických reportů</li> </ul> <p>Součinnost se 3. stranami</p> <ul style="list-style-type: none"> <li>• v rámci zajištění podpory 2. úrovně zabezpečovat komunikaci se 3. stranami v případě záručních oprav, řešení problémů či nestandardních požadavků na změny</li> </ul>
--	--

	<ul style="list-style-type: none"> <li>• Komunikace se třetími stranami bude probíhat prostřednictvím e-mailu a telefonu.</li> </ul> <p>Správa RSA klíčenek pro MD – evidence, obměna, výdeje (řádově stovky)          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</p> <p>Dodavatel se zavazuje předat informace a dokumentaci dle článků 17 a 18 Smlouvy, dodržovat principy ITIL a je povinen zajistit účast expertů na jednání, pokud si je Objednatel vyžádá.</p>									
Dostupnost služby	<p>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 Objednatelům do jeho přijetí 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“</p> <table border="1" data-bbox="475 981 1423 1171"> <thead> <tr> <th>Služba</th> <th>Příjem</th> <th>Rozsah zaručeného provozu služby</th> </tr> </thead> <tbody> <tr> <td>Příjem kontaktů e-mailem</td> <td>7x24</td> <td>Pracovní dny 7:00-18:00</td> </tr> <tr> <td>Příjem telefonických kontaktů</td> <td>Pracovní dny 7:00-18:00</td> <td>Pracovní dny 7:00-18:00</td> </tr> </tbody> </table> <p>Mimo „Rozsah zaručeného plnění provozu služby“ zajistí Dodavatel 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 Dodavatel Objednateli ke dni účinnosti této smlouvy a o případných změnách bude Objednatel informovat minimálně s měsíčním předstihem. Pro tuto linku neplatí parametry Dostupnosti a SLA uváděné následně v tomto katalogovém listu.</p> <p>Dostupnost služby měsíční: 98%.</p> <p>Maximální doba jednoho výpadku: 120 minut.</p> <p>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.</p> <p>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 Dodavatel, 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</p>	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
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								

	<p>výpočtu dostupnosti promítnou i plánované odstávky, pokud se uskutečnily v období zaručeného provozu služby. Dostupnost bude uvedena v %.</p> $\text{Dostupnost} = (PD_{\text{období}} - N_{\text{služby}}) / PD_{\text{období}} * 100 [\%]$ <p>Kde:</p> <p><math>PD_{\text{období}}</math> .... celkový rozsah zaručeného provozu služby doby za sledované období</p> <p><math>N_{\text{služby}}</math> ..... Doba úplné nedostupnosti služby ve sledovaném období, za níž odpovídá Dodavatel</p> <p>Pro určení slevy za nedodržení dostupnosti je rozhodující jak „Maximální doba jednoho výpadku služby“, tak „Dostupnost služby měsíční“.</p> <p>Za každé překročení maximální doby jednoho výpadku služby je poskytnuta sleva v souladu se Smlouvou v prioritě 1.</p> <p>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.</p> <p>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.</p>
SLA	<p>U 90% nahlášených Incidentů / Servisních požadavků za sledované období musí být Doba reakce:</p> <p>Pro období: pracovní dny 7:00-18:00 (pracovní doba)</p> <ul style="list-style-type: none"> <li>• 15 minut pro nahlášení telefonem;</li> <li>• 30 minut pro nahlášení e-mailem.</li> </ul> <p>Pro období mimo pracovní dobu:</p> <ul style="list-style-type: none"> <li>• Následující pracovní den do 7:30 hodin</li> </ul> <p>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.</p> <p>Plnění v %:</p> $\text{Plnění} = (PI - PNI) / PI * 100 [\%]$ <p>Kde: PI .... počtu všech nahlášených Incidentů / Servisních požadavků za sledované období</p>

	<p style="text-align: center;">PNI ..... počet překročených Dob reakce za sledované období</p> <p>Pro určení slevy za nedodržení doby reakce je rozhodující „Plnění v %“.</p> <p>Pokud je Doba reakce větší nebo rovna 90%“, sleva na jednotlivé překročení doby reakce se neuplatňuje.</p> <p>Pokud je skutečné plnění menší než 90%“, sleva se uplatňuje, a to pro každé jednotlivé překročení doby reakce, tj. slevy se sčítají. Za každých započatých 10% překročení SLA se uplatňuje sleva ve výši hodnoty odpovídající Prioritě 1.</p> <p>Při výpadku služby je Dodavatel povinen bezodkladně informovat Objednatele o výpadku, o obnovení služby; dále je Dodavatele povinen:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> </ul>
Možnost plánovaných odstávek	Mimo pracovní dobu a po dohodě s Objednatelem.

## 5 Služba převzetí provozu – KL005

Kód služby	<b>KL005</b>
Název služby	<b>Služba převzetí provozu</b>
Cíl služby	Cílem služby je zajistit u Dodavatele potřebnou infrastrukturu nutnou k poskytování služeb KL001-KL004 Dodavatelem a zajistit migraci provozu aplikací na tuto Dodavatelovu infrastrukturu z infrastruktury předchozího dodavatele služeb
Popis služby	<p>Služba musí zajistit migraci, která se skládá:</p> <ol style="list-style-type: none"> <li>1. Z přípravného období, ve kterém musí Dodavatel zajistit vytvoření SW a HW prostředí pro následný provoz služeb v rozsahu a kvalitě, které vyžaduje provoz KL 001 až KL004.</li> <li>2. Z návrhu reálného harmonogramu přechodu prostředí, aplikací, licencí a dalších komponent nezbytných pro provoz služeb, který bude realizován dle těchto zásad: <ol style="list-style-type: none"> <li>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 dodavatele podpory provozu aplikací (součinnost/změny) minimálně 45 kalendářních dní předem, nedohodne-li se Dodavatel s Objednatelem na kratším termínu.</li> <li>b. Pokud budou přechody rozděleny do dílčích přechodů realizovaných v různých termínech, bude pro každý takový dílčí přechod stanoven dílčí harmonogram.</li> <li>c. Harmonogram(y) a jejich případné úpravy budou schvalovány Objednatelem.</li> <li>d. Součinnost dodavatele podpory provozu aplikace bude spočívat pouze v otestování úspěšnosti přechodu, v konzultaci, případně ve změně IP adres (bude-li to nezbytně nutné).</li> <li>e. Součástí přechodu (dílčího přechodu) musí být testovací scénář pro provozovatele aplikací (aplikace).</li> <li>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.</li> <li>g. Každému přechodu musí předcházet test přechodu, resp. test dílčího přechodu. Požadavky na opakované testování dodavatelem podpory provozu aplikace z důvodu problémů způsobených Dodavatelem nebudou Objednatelem Dodavateli hrazeny a vznikne-li nárok na úhradu ze strany dodavatele podpory provozu aplikace, musí být vypořádány Dodavatelem,</li> </ol> </li> </ol>

	<p>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 Dodavateli.</p> <p>3. Přejít aplikací do cílového stavu má stanovenu maximální dobou odstávky:</p> <p>a. Pro kategorie KIS a VIS dle vyhlášky č. 317/2014 Sb. - 12 hodin o víkendu</p> <p>b. Pro ostatní systémy – 36 hodin o víkendu</p> <p>4. Provoz již převedeného(ných) systému(ů) do doby plného ukončení tohoto KL s SLA stanovenými v KL001-KL004.</p> <p>5. Spolupráci se stávajícím (současným) provozovatelem IT infrastruktury (O2 IT Services, s.r.o.) v rozsahu jeho Exit plánu (dle smlouvy S-239-330/2015 zveřejněné na profilu zadavatele)</p> <p>6. Dodavatel musí umožnit kontrolu ze strany Objednatele v rozsahu stanoveném Smlouvou, a to i za využití 3. stran, které Objednatelem kontrolou pověří.</p> <p>7. Dodavatel musí na vlastní náklady veškeré nezbytné licence k převzetí služby.</p>
<b>Rozsah zaručeného provozu služby</b>	
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



## 6 Služba předání provozu – KL006

Kód služby	<b>KL006</b>
Název služby	<b>Služba předání provozu</b>
Cíl služby	Cílem služby je zajistit migraci provozu aplikací na infrastrukturu provozovaných Dodavatelem k jinému dodavateli služeb nad rámec povinností čl. 17 Smlouvy
Popis služby	<p>Služba musí zajistit nad rámec povinností obsažených v ostatních katalogových listech, resp. v čl. 17 Smlouvy součinnost tak, aby nedošlo k ohrožení provozu předávaných agend. Služba je určena zajištění součinnosti Dodavatele na předání služeb v oblastech, které nelze v okamžiku podpisu této smlouvy přesně popsat a je zaměřena především na tyto oblasti:</p> <ol style="list-style-type: none"> <li>1. Poskytnout novému provozovateli infrastruktury veškeré potřebné informace (i ty, které vzniknou v průběhu plnění smlouvy a nejsou popsány v čl. 17 a 18 Smlouvy)</li> <li>2. Umožnit migraci dat, konfigurací, licencí i aplikací a spolupracovat s Objednatelem a 3. stranami tak, aby nedocházelo k zbytečným zpožděním, výpadkům a odstávkám.</li> </ol>
<b>Rozsah zaručeného provozu služby</b>	
Kompletní realizace do termínů stanovených smlouvou	
SLA	Splnění v termínech a rozsazích Smlouvy
Možnost plánovaných odstávek	N/A

## 7 Služba na vyžádání – KL007

Kód služby	<b>KL007</b>
Název služby	<b>Služba na vyžádání</b>
Cíl služby	Cílem této služby je umožnit realizaci požadavků Objednatele v závislosti na potřebách provozovaných aplikací, bezpečnosti a technologickém vývoji
Popis služby	<p>Služba umožňuje zajistit činnosti nad rámec katalogových listů KL001-KL006 v závislosti na potřebách Objednatele, které Objednatel nemohl předvídat, resp. přesně popsat v okamžiku uzavření Smlouvy. Jedná se o činnosti, které souvisejí se službami popsány v KL001-KL006 a které nelze především z důvodů technologických, bezpečnostních či z důvodů požadavku odpovědnosti za SLA zajistit jiným dodavatelem.</p> <p>Služby na vyžádání se objednávají po dohodě Dodavatele a Objednatele. Dodavatel 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.</p> <p>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.</p>
<b>Rozsah zaručeného provozu služby</b>	
Dle dohody stanovené objednávkou	
SLA	Splnění v termínech a rozsazích Smlouvy
Možnost plánovaných odstávek	N/A

## 8 SEZNAM ZKRATEK

ADR	Aplikace Registr nebezpečných nákladů
CRŘ	Aplikace Centrální registr řidičů
ČKP	Česká kancelář pojistitelů
ČR	Česká republika
DB	Databáze
DC	Datové centrum
DPH	Daň z přidané hodnoty
DSA	Dopravně správní agendy
DT	Aplikace Digitální tachograf
HZS	Hasičský záchranný systém
IMIS	Integrovaný manažerský informační systém (tvořen IFS a EGJE aplikací)
IS	Informační systém
IS NP	Informační systém námořní plavby
IS TP	Informační systém technických prohlídek (dříve CIS-STK - Centrální informační systém stanic technické kontroly)
L2	2. datová vrstva OSI modelu (Open System Interconnection Reference Model)
MD	Ministerstvo dopravy ČR
MS	Společnost Microsoft
ORP	Obec s rozšířenou působností
OS	Operační systém
OSS	Organizační složky státu
PČR	Policie České republiky
RPSD	Registr podnikatelů v silniční dopravě
RSV	Aplikace Registr silničních vozidel (dříve CRV – Centrální registr vozidel)
ŘV	Řídící výbor

### Cizí zkratky

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
O2 MBR	O2 Managed Backup and Restore

02 MDS	Služba O2 Managed Data Storage
OTRS	Opensource Ticket Request System
RAC	Real Application Cluster
RAM	Random Access Memory
SAN	Storage Area Network
SD	Service Desk
SIEM	Security Information and Event Management
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 Network
VPN	Virtual Private Network

## Příloha č. 2

### Specifikace ceny

Služba	Označení katalogového listu	Cena služby za 1 měsíc v Kč bez DPH	Cena služby v Kč za 1 měsíc s DPH 21%
Služba bezpečnostní politiky	KL001	281.987,00	341.204,27
Služba technického provozu a poskytování virtuální infrastruktury	KL002	2.816.384,00	3.407.824,64
Služba provozu CRŘ	KL003	81.565,00	98.693,65
Služba provozu Call Centra	KL004	45.600,00	55.176,00
<b>CELKEM za KL001-KL004</b>	-----	<b>3.225.536,00</b>	<b>3.902.898,56</b>

Služba	Označení katalogového listu	Maximální cena za provedení služby v Kč bez DPH	Maximální cena za provedení služby v Kč s DPH 21%
Služba převzetí <sup>1)</sup>	KL005	8.559.921,00	10.357.504,41
Služba předání <sup>2)</sup>	KL006	2.853.307,00	3.452.501,47
<b>Celkem za KL005-KL006</b>	-----	<b>11.413.228,00</b>	<b>13.810.005,88</b>

- <sup>1)</sup> Tato služba bude hrazena na základě Objednateli doložené a oprávněné fakturace Dodavatele v cenách v místě obvyklých nutných k zajištění činnosti přebírání služeb dle KL001-KL004 (nikoliv však náklady na zajištění schopnosti služby provozovat), avšak maximálně do výše zde uvedené.
- <sup>2)</sup> Tato služba bude hrazena na základě Objednateli doložených reálných nákladů Dodavatele nutných k činnostem předání služeb dle KL001-KL004, avšak maximálně do výše zde uvedené.

Služba	Označení katalogového listu	Maximální cena za 1 člověkodenní v Kč bez DPH	Maximální cena za 1 člověkodenní v Kč s DPH 21%
Služba na vyžádání <sup>3)</sup>	KL007	5.400,00	6.534,00

- <sup>3)</sup> 1 člověkodenní odpovídá 8 hodinám práce jedné osoby.