ČÍSLO SMLOUVY MF

23/906/0039/01

DODATEK Č. 1

KE SMLOUVĚ NA POSKYTOVÁNÍ SLUŽEB BEZPEČNÉHO DATOVÉHO CENTRA

(evidovaná u Objednatele pod č. 9006/065/2023, evidovaná u Poskytovatele pod č. SML2023143, č. j. SPCSS-08820/2023)

uzavřené dne 28. 3. 2024 (dále jen „**Smlouva**")

(evidovaný u Objednatele pod č. 9006/014/2025, evidovaný u Poskytovatele pod č. SML2023143_Dodatek č.1, č. j. SPCSS-00717/2025)

(to vše dále jen „**Dodatek**")

Česká republika – Ministerstvo financí
se sídlem: Letenská 15, 110 00 Praha 1
za niž jedná: xxxxxxxxxx, xxxxxxxxxx
IČO: 00006947
DIČ: CZ00006947
ID datové schránky: xzeaauv
bankovní spojení: Česká národní banka
číslo účtu: 3328001/0710
(dále jen „**Objednatel**" nebo „**MF**")

a

Státní pokladna Centrum sdílených služeb, s. p.
se sídlem: Na Vápence 915/14, 130 00 Praha 3
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 76922
zastoupený: xxxxxxxxxx, xxxxxxxxxx
IČO: 03630919
DIČ: CZ03630919
ID datové schránky: ag5uunk
bankovní spojení: Česká národní banka
číslo účtu: 206201/0710
(dále jen „**Poskytovatel**" nebo „**SPCSS**")

(Objednatel a Poskytovatel dále též jen samostatně jako „**Smluvní strana**" nebo společně jen „**Smluvní strany**").

VZHLEDEM K TOMU, ŽE

(A) Dne 28. 3. 2024 byla mezi SPCSS a MF uzavřena výše uvedená Smlouva;

(B) Smluvní strany se dohodly, že tímto Dodatkem změní rozsah plnění dle Smlouvy a v návaznosti na to učiní nezbytné změny Smlouvy;

SE SMLUVNÍ STRANY DOHODLY TAKTO:

I. PŘEDMĚT DODATKU

1.1 Na základě čl. XVII odst. 17.11 Smlouvy se Smluvní strany dohodly, že ruší původní znění Přílohy č. 1 – Technická specifikace Služeb Smlouvy a nahrazují je jejím novým zněním, které je nedílnou součástí tohoto Dodatku jako jeho Příloha č. 1.

II. ZÁVĚREČNÁ USTANOVENÍ

2.1 Tento Dodatek nabývá platnosti dnem podpisu všemi Smluvními stranami a účinnosti dnem zveřejněním v registru smluv podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů nebo od 1. 4. 2025, podle toho, která ze skutečností nastane později. Objednatel se zavazuje, že Dodatek zveřejní v registru smluv.

2.2 Ostatní ustanovení Smlouvy nedotčená tímto Dodatkem, zůstávají v platnosti beze změn.

2.3 Dodatek je vyhotoven v elektronické podobě v 1 vyhotovení v českém jazyce s elektronickými podpisy všech Smluvních stran v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

2.4 Smluvní strany souhlasí s tím, že označování dokumentů vzniklých na základě tohoto Dodatku bude probíhat v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.first.org/tlp/). Dokumenty budou označeny příznakem, který stanoví podmínky použití informací v těchto dokumentech.

2.5 Nedílnou součást Dodatku tvoří tyto přílohy:

Příloha č. 1 – Příloha č. 1: Technická specifikace Služeb

2.6 Smluvní strany prohlašují, že se seznámily s obsahem Dodatku a že tento Dodatek byl sepsán dle jejich pravé a svobodné vůle, nikoliv v tísni či za nápadně nevýhodných podmínek, na důkaz toho připojují své podpisy.

Za Objednatele:			Za Poskytovatele:		
V Praze	dne	dle elektronického podpisu	V Praze	dne	dle elektronického podpisu

xxxxxxxxxx xxxxxxxxxx Česká republika – Ministerstvo financí	xxxxxxxxxx xxxxxxxxxx Státní pokladna Centrum sdílených služeb, s. p.

KATALOG SLUŽEB
BEZPEČNÉHO DATOVÉHO CENTRA

Obsahem katalogu služeb bezpečného datového centra jsou jednotlivé katalogové listy, které obsahují popis parametrů a podmínek poskytování služeb bezpečného datového centra. Katalog obsahuje následující katalogové listy (dále také „KL"):

Seznam Katalogových listů			
Označení	**Název**	**Termíny poskytování služby**	
		zahájení	**ukončení**
MF/01	Zajištění a provoz produkčního prostředí IISSP	01.04.2024	31.03.2028
MF/02	Hosting aplikace Monitor	01.04.2024	31.03.2028
MF/03	Provoz informačních portálů	01.04.2024	31.03.2028
MF/04	Kapacita HSM (Hardware Security Module)	01.04.2024	31.03.2028
MF/05	Zajištění a provoz produkčního prostředí APAO	01.04.2024	31.03.2028
MF/06	Zajištění a provoz produkčního prostředí AISG	01.04.2024	31.03.2028
MF/07	Zajištění a provoz produkčního prostředí EESS	01.04.2024	31.03.2028
MF/08	Zajištění a provoz produkčního prostředí ARES	01.04.2024	31.03.2028
MF/09	Zajištění a provoz produkčního prostředí OPEN DATA	01.04.2024	31.03.2028
MF/10	Housing DWDM	01.04.2024	31.03.2028
MF/11	Zajištění a provoz produkčního prostředí pro IS FORM	01.04.2025	31.03.2028

MF/01	Zajištění a provoz produkčního prostředí IISSP

1 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba bude poskytována v režimu 7x24 hodin. Celková doba je rozdělena na dvě části, běžnou provozní dobu (v kalendářních dnech od 6:00 hod do 20:00 hod) a rozšířenou provozní dobu (v kalendářních dnech od 20:00 hod do 6:00 hod).

Prostředí testování třetích stran a školení bude poskytováno pouze v režimu 5x8 hodin ve zkrácené provozní době, tj. v pracovních dnech od 08:00 hod do 16:00 hod.

2 POPIS ROZSAHU SLUŽBY

Obsahem služby Zajištění a provoz produkčního prostředí IISSP v režimu podle odst. 1 tohoto Katalogového listu je zajištění bezpečného produkčního prostředí IISSP a jeho spolehlivého provozu. V termínu zahájení poskytování služby Provoz IISSP podle tohoto katalogového listu má MF k dispozici HW infrastrukturu produkčního prostředí pro provoz IISSP, která je popsána v jednotlivých oblastech služby.

Oblast – Infra služby

2.1 Poskytování výpočetního výkonu a zálohovacích kapacit

Služba bude realizována prostřednictvím virtuálních serverů, které mají dostatečný výpočetní výkon pro IISSP a požadovanou dostupnost.

Koncepce HW architektury a layout prostředí IISSP splňuje následující požadavky:

- celé primární prostředí nemusí být provozováno v jediném prostoru:
  - architektura umožňuje provozní režim, kdy jsou mezi prostory standardně (tedy pomocí administrátorských nástrojů bez nutnosti rekonfigurace prostředí) přesouvány celé aplikace (celá vertikála – tedy všechny vrstvy aplikace). Výjimkou může být volná topologie pro aplikační servery, ke kterým je přístup balancován na úrovni přístupové vrstvy – takové aplikační servery pak mohou být provozovány v libovolné lokaci bez ohledu na to, kde je aktuálně provozována primární vrstva aplikace;
  - architektura podporuje provoz komponent IISSP v obou prostorech paralelně, každá komponenta (míněno v rozsahu všech jejích vrstev) pak má "záložní" centrum v prostoru, kde není "standardně" provozována (prostory se jistí vzájemně);
- architektura infrastruktury umožňuje pro všechny prvky (servery, storage i komunikace) standardní rozšiřitelnost vertikálně i horizontálně s minimálním dopadem na provoz;
- přístup k bez stavovým aplikačním serverům je řízen balancováním (pokud to aplikace umožňuje) – proto mohou být aktivovány na každém dostupném hostitelském serveru obou prostor.

Součástí poskytování výpočetního výkonu a zálohovacích kapacit pro zajištění a provoz produkčního prostředí IISSP není poskytnutí jakýchkoliv licencí, podlicencí ani sekundárních podlicencí pro MF.

2.1.1 Výpočetní výkon na platformě Power

Výpočetní výkon na RISC platformě Power je poskytován na technologii platformy Power8 a vyšší.

V každém datovém centru jsou umístěny servery pSeries. Jednotlivé servery mají minimálně 2 CPU sockety.

Platforma výpočetního výkonu nemá interní disky, je připojena ke službám poskytování diskových prostorů (definice služeb poskytování diskového prostoru STOR1). Konektivita k diskovému úložišti je zajištěna pomocí redundantního FibreChannel (FC) propojení.

V ceně služby je zahrnuto i umístění v datovém centru včetně racku a energie.

2.1.2 Výpočetní výkon na platformě x64

Výpočetní výkon na platformě x64 je poskytován na technologiích Intel Xeon E5-2630 v4 a vyšší skrze optimalizované virtuální servery s operačními systémy Windows nebo Linux.

V ceně služby je zahrnuto i umístění v datovém centru včetně racku a energie.

Alokace je realizována prostředky virtualizační platformy a je v odpovědnosti Poskytovatele infrastruktury.

2.1.3 Celkové výkonnostní parametry prostředí IISSP jsou uvedeny v následující tabulce:

<table>
<tr><th colspan="4">Prostředí pro provoz IISSP – Platforma Power</th></tr>
<tr><th>Prostředí</th><th>CPU</th><th>RAM (GB)</th><th>Diskový prostor (GB)</th></tr>
<tr><td>Produktivní</td><td colspan="3" rowspan="5">Celkový poskytovaný výkon pro jednotlivá prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy).</td></tr>
<tr><td>Pre-produktivní</td></tr>
<tr><td>Testovací</td></tr>
<tr><td>Vývojové</td></tr>
<tr><td>Testování třetích stran a školení</td></tr>
<tr><td>Celkový rezervovaný výkon</td><td>184,5</td><td>4 021</td><td>186 402</td></tr>
<tr><th colspan="4">Prostředí pro provoz IISSP – Platforma x64</th></tr>
<tr><th>Prostředí</th><th>vCPU</th><th>vRAM (GB)</th><th>Diskový prostor (GB)</th></tr>
<tr><td>Produktivní</td><td colspan="3" rowspan="5">Celkový poskytovaný výkon pro jednotlivá prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy).</td></tr>
<tr><td>Pre-produktivní</td></tr>
<tr><td>Testovací</td></tr>
<tr><td>Vývojové</td></tr>
<tr><td>Testování třetích stran a školení</td></tr>
<tr><td>Celkový rezervovaný výkon</td><td>6</td><td>28</td><td>381</td></tr>
</table>

2.1.4 Poskytování zálohovacích kapacit

Způsob realizace zálohování respektuje požadavky na dostupnost, výkonnost a umožňuje využít možnosti HW a technologií produkčního prostředí IISSP, zejména diskových polí a páskových knihoven. Zálohovací systém realizuje zálohování stanoveným způsobem a režimem nutným k zajištění SLA. Standardem je zálohování operačních systémů, vybraných souborových systémů a databází.

Požadavky na RPO, RTO a zálohovací plány jsou uvedeny v provozní dokumentaci a jsou schvalovány řídícími orgány provozu.

Oblast – Provozní služby

2.2 Poskytování správy, servisní podpory SW a údržby HW

2.2.1 Poskytování správy operačních systémů

Služba je poskytována na následujících operačních systémech:

- MS Windows: MS Windows Server Datacenter 2019 a vyšší;
- IBM AIX 7 a vyšší;
- Linux: Red Hat Enterpise Linux 7.0 či vyšší nebo jiná distribuce založená na Red Hat, která je k dispozici bez podpory.

Předpokladem služby pro licencované operační systémy je zajištění licence a maintenance OS.

Součástí služby není implementace a správa aplikačních komponent operačních systémů, respektive aplikačního SW přibaleného k základnímu OS, jako jsou například web servery, aplikační servery, middleware, databáze nebo adresářové služby pro účely správy aplikačních uživatelů.

Služba zahrnuje následující činnosti:

- administrace operačních systémů, tzn. incident management, problem management a change management (vyjma změn aplikačních komponent – viz výše);
- aktualizace operačních systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost aplikací;
- kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;
- provádění restartů operačních systémů dle požadavků Objednatele;
- změny konfigurací OS;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- profylaxe systému dle harmonogramu v měsíčních intervalech;
- součinnosti s případnou instalací a konfigurací nového software;
- instalace a údržba certifikátů doporučených dodavatelem aplikace pro zabezpečení přístupů na servery;
- správa lokálních uživatelských účtů v OS;
- úpravy výkonnostních parametrů systému;
- správa souborového systému (filesystem, přístupová práva a zaplněnost);
- testování změn provedených v OS;
- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);
- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele probíhá formou nástrojů typu sudo

nebo jsou řízeny pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;

- aplikační adresáře s rostoucím objemem dat (logy, databáze, úložiště souborů) jsou umístěny na samostatných diskových prostorech (volume, logický disk);
- Poskytovatel instaluje vždy minimální výchozí instalaci operačního systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace (balíčky, filesystemy, úpravy v konfiguračních souborech).

2.3 Zajišťování provozu bezpečného komunikačního rozhraní

V rámci zajišťování provozu bezpečného komunikačního rozhraní jsou typicky čerpány následující aktivity:

- připojení řešení z datových center SPCSS do internetu. Internetová konektivita je primárně realizována připojením do dvou nezávislých uzlů NIX dvěma nezávislými optickými trasami o kapacitě 10 Gbps a sekundárně připojením dvěma nezávislými linkami 100 Mbps přes ISP;
- připojení řešení z datových center SPCSS do GOVBONE a CMS2. Připojení je zajištěno redundantními propoji v rámci DC SPCSS;
- propojení datových center DC Vápenka a DC Zeleneč – DCI;
- firewall a IPS;
- aplikační firewall a loadbalancer F5;
- VPN – vzdálené připojení do sítě SPCSS pomocí VPN, a to buď jako site-to-site VPN nebo remote-access VPN. Určeno pro dodavatele pro účely vzdálené správy aplikace.

Součástí výše uvedených položek je následující podpůrná infrastruktura a související služby, které jsou nezbytné pro provoz bezpečného propojení:

- plně redundantní síťová infrastruktura Poskytovatele;
- ochrana proti DoS a DDoS útokům;
- přiřazení a aktualizace bezpečnostních oprávnění uživatelům a zařízením v síti;
- aktualizace a opravy prvků síťové infrastruktury;
- vyhodnocování a optimalizace výkonu sítě a síťových prvků;
- zajištění dokumentace poskytovaných služeb a jejich technického nastavení pro potřeby Objednatele v takovém rozsahu, aby Objednatel byl schopen dokumentovat správu a provoz aplikační vrstvy ve všech provozních stavech podporovaných aplikací;
- řízení provozu a dohled nad kvalitou poskytované služby;
- řízení provozu a dohledu nad kvalitou poskytované služby vychází z požadavků příslušných standardů ITIL a norem ČSN ISO/IEC 20000.

2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb

2.4.1 Řízení provozu Systému zahrnuje zejména:

- koordinaci provozu HW a SW;
- řízení v oblasti rizik a kvality;
- řízení komunikace mezi stranami, které se účastní poskytování služby;
- koordinaci změnových řízení v rámci poskytování služby;
- personální zajištění řízení provozu služby zahrnuje obsazení role vedoucího provozu služby;

2.4.2 Podpora poskytování služby prostřednictvím SW nástrojů SPCSS zahrnuje zejména:

- poskytování informací pro posouzení postupu řešení nedostupnosti a závad služby;
- procesní řízení získaných informací;
- SW a personální zajištění.

2.4.3 Dohled nad kvalitou poskytované služby zahrnuje zejména:

- trvalý provozní a bezpečnostní dohled;
- vyhodnocování SLA specifikované v Katalogovém listu.

IISSP musí splňovat veškeré požadavky na informační systém Kritické informační infrastruktury dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), včetně dalších požadavků prováděcích předpisů a nařízení, zejména Směrnice SŘBI MF. SPCSS je ve vztahu k MF významným dodavatelem a provozovatelem IISSP.

Bezpečnost a dohledy na úrovni infrastruktury obsahuje bezpečnostní a provozní dohled na úrovni odpovídající charakteru části služby:

- poskytování výpočetního výkonu;
- poskytování správy operačních systémů;
- zajišťování provozu bezpečného komunikačního rozhraní.

Pravidelným měsíčním výstupem bezpečnostního dohledu jsou informace o kybernetické bezpečnosti infrastruktury IISSP, která je integrální součástí zprávy – Detail bezpečnostního monitoringu IISSP, která je zpracovávána v souladu se Smlouvou o podpoře a rozvoji IISSP a poskytování souvisejících služeb, tato zpráva dále také obsahuje informace o kybernetické bezpečnosti infrastruktury služeb podle této přílohy MF/02 Hosting aplikace Monitor a MF/ 04 – Kapacita HSM.

Poskytovatel se zavazuje tímto plnit povinnosti, které vychází ze shora uvedené legislativy.

Poskytovatel je povinen při poskytování infrastrukturních služeb plně implementovat a provádět ustanovení ZoKB a VoKB, zejména:

- zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému Kritické informační infrastruktury a vést o nich bezpečnostní dokumentaci;
- provádět opatření dle § 11 ZoKB;
- vést veškeré provozní a bezpečnostní záznamy infrastruktury, realizovat organizační a technická opatření požadovaná MF ke sběru a vyhodnocování záznamů dle vyhlášky č. 82/2018 Sb. vlastními prostředky;
- informovat Manažera kybernetické bezpečnosti MF o zranitelnostech, hrozbách a rizicích a jejich zvládání a pravidelných revizí;
- hlásit Manažeru kybernetické bezpečnosti MF a informovat bezpečnostního správce tohoto systému o bezpečnostních hlášeních, kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech bez zbytečného odkladu;
- hlásit kybernetické bezpečnostní incidenty na Národní úřad pro kybernetickou a informační bezpečnost formou požadovanou VoKB a Manažera kybernetické bezpečnosti MF informovat a hlášení KBI na NÚKIB bez zbytečného odkladu o kybernetických bezpečnostních incidentech, a to bezodkladně po jejich detekci;
- realizovat bezpečnostní opatření ke zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů po konzultaci s Manažerem kybernetické bezpečnosti MF;
- umožnit přístup pro určené osoby Objednatele k řešení tiketů do systému Service Desk Poskytovatele, Manažerovi kybernetické bezpečnosti MF nebo dalším určeným osobám vzdálený přístup k záznamům týkajícím se IISSP v nástroji SIEM;
- nakládat s daty IISSP, která budou smazána v souladu s jejich účelem a dodržovat pravidla pro likvidaci dat;
- v rozsahu IISSP dodržovat Směrnice MF a realizovat bezpečnostní opatření ve formě organizačních a technických opatření i na SPCSS;
- komunikovat s MF kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty v rozsahu poskytovaných služeb nebo rozsahu, který by ovlivňoval poskytované služby;

- řídit bezpečnostní rizika IISSP;
- řídit kontinuitu provozu IISSP;
- předávat předem dohodnutou formou data, provozní údaje a informace vyžádané Objednatelem;
- řídit změny IISSP.

3 KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

3.1 Požadovaná měsíční dostupnost oblastí služby

Prostředí	Dostupnost oblastí služby	
	Poskytování výpočetního výkonu a zálohovacích kapacit	Zajišťování provozu bezpečného komunikačního rozhraní
Produktivní	99,5 %	99,5 %
Pre-produktivní	95,0 %	95,0 %
Vývojové	95,0 %	95,0 %
Testovací	95,0 %	95,0 %
Testování třetích stran a školení	95,0 %	95,0 %

Nedostupnost služby způsobená hardwarovou nebo jinou technickou závadou infrastruktury produkčního prostředí pro provoz IISSP (dále jen „PPSP") se počítá od okamžiku zahájení nedostupnosti systému IISSP pro koncové uživatele do okamžiku odstranění této závady. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti systému IISSP pro koncové uživatele, počítá se nedostupnost služby od doby jejího nahlášení do Service Desku SPCSS.

Nedostupnost služby způsobená softwarovou závadou infrastruktury PPSP (nastavení systému, pravidla a prostupy firewalu, apod.) se počítá od okamžiku nahlášení nedostupnosti systému IISSP pro koncové uživatele do okamžiku odstranění této závady.

Za **nahlášení nedostupnosti služby** se považuje založení odpovídajícího servisního hlášení v aplikaci **Service Desk SPCSS** (servicedesk.spcss.cz).

Dostupnost služby se vypočítá podle následujícího vzorce:

kde

$$D = 100 \times \frac{T - N}{T}$$

D je dostupnost [%] v daném období.

T vyjadřuje fond provozní doby služby v daném období.

N vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky schválené mimořádné odstávky.

Servisní okna poskytované služby jsou v době plánované odstávky, zveřejněné vždy předem ve formě Plánu odstávek na kalendářní rok, případně ve čtvrtek od 20:00 do 6:00 vyjma čtvrtka před plánovanou odstávkou. Pokud budou mít činnosti v servisním okně dopad do dostupnosti, bude Poskytovatel žádat o jejich schválení formou mimořádné odstávky.

3.2 Požadované lhůty pro obnovení služby

Prostředí	Lhůta pro obnovení služby v běžné provozní době v hodinách

	Incident kategorie A	Incident kategorie B	Incident kategorie C
Produktivní	4	6	24
Pre-produktivní	24	72	168
Vývojové	24	72	168
Testovací	24	72	168
Prostředí	**Lhůta pro obnovení služby ve zkrácené provozní době v hodinách**		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Testování třetích stran a školení	40	72	168

Kategorizace incidentů:

Incident kategorie A	Služba není použitelná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje jeho užívání většině nebo všem jejím uživatelům. Tento stav kritickým způsobem ohrožuje běžný provoz Objednatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody, a při tom neexistuje náhradní způsob zajištění poskytování služeb tohoto systému.
Incident kategorie B	Služba, je ve svých funkcích degradována tak, že tento stav zásadně omezuje běžný provoz Objednatele.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

3.3 Požadované lhůty pro obnovení služby pro vybrané komponenty

Lhůty pro obnovení služby v produktivním prostředí provozovaném v době konání plánovaného a odsouhlaseného Disaster Recovery testu (komponenty služby 2.1 Poskytování výpočetního výkonu a zálohování a 2.3 zajišťování provozu bezpečného komunikačního rozhraní) jsou stejné jako v testovacím prostředí, tedy:

Prostředí	Lhůta pro obnovení služby v běžné provozní době v době konání plánovaného a odsouhlaseného Disaster Recovery testu		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Produktivní	24	72	168

4 CENA SLUŽBY

Rozdělení služby dle odst. 2 tohoto katalogového listu	Měsíční cena v Kč (MF/01)		
	bez DPH	DPH	s DPH
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	5 299 291,00	1 112 851,11	6 412 142,11
2.2 Poskytování správy, servisní podpory SW a údržby HW (Provozní služba)	1 078 432,00	226 470,72	1 304 902,72
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	2 003 572,00	420 750,12	2 424 322,12
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	439 097,00	92 210,37	531 307,37
Celková měsíční cena	**8 820 392,00**	**1 852 282,32**	**10 672 674,32**

5 SMLUVNÍ POKUTY ZA NESPLNĚNÍ KVALITATIVNÍCH PARAMETRŮ POSKYTOVÁNÍ SLUŽBY

Za porušení kvalitativních parametrů, nedodržení dostupnosti služby dle pododst. 3.1 a nedodržení požadované lhůty pro obnovení služby dle pododst. 3.2 a pododst. 3.3, je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu vypočítanou za jednotlivé oblasti služby dle odst. 2 tohoto katalogového listu.

Název parametru	Smluvní pokuta za porušení parametru služby v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Max. výše smluvní pokuty v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Způsob výpočtu
Dostupnost oblasti Služby	1	40	za každých započatých 15 minut nad povolený limit nedostupnosti nebo doby vyřešení incidentu
Doba vyřešení incidentu kategorie A	1	40	
Doba vyřešení incidentu kategorie B	0,5	15	
Doba vyřešení incidentu kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období.

Výše smluvní pokuty se při nedodržení dostupnosti konkrétního prostředí nebo nedodržení doby vyřešení incidentu vypočítá jako procento z celkové měsíční ceny služby dle tabulky v odst. 4 tohoto katalogového listu.

MF/02	Hosting aplikace Monitor

1 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba bude poskytována v provozní době 24x7 hodin.

Celková doba je rozdělena na dvě části, běžnou provozní dobu (v kalendářních dnech od 6:00 hod do 20:00 hod) a rozšířenou provozní dobu (v kalendářních dnech od 20:00 hod do 6:00 hod).

2 POPIS ROZSAHU SLUŽBY

Obsahem služby je zajištění bezpečného produkčního prostředí Informačních portálů MF ČR a jeho spolehlivého provozu pomocí cloudových Služeb SPCSS (Google Cloud platform).

<table>
<tr><th colspan="4">Prostředí pro provoz informačních portálů – MONITOR – Platforma x64</th></tr>
<tr><th>Prostředí</th><th>CPU</th><th>RAM (GB)</th><th></th></tr>
<tr><td>Produktivní</td><td colspan="3" rowspan="3">Celkový rozsah pro obě prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy).</td></tr>
<tr><td>Pre-produktivní</td></tr>
<tr><td>Testovací</td></tr>
<tr><td>Celkový rezervovaný výkon</td><td colspan="3">4 000 kreditů</td></tr>
</table>

Oblast – Cloudové služby

2.1 Poskytování výpočetního výkonu

Služba je realizována prostřednictvím cloudových Služeb SPCSS (Google Cloud platform). Architektura prostředí je designována, co se výkonu týká, jako dynamicky škálovatelná a maximálně využívá webapp cloudových Služeb SPCSS (Google Cloud platform).

Poskytování správy cloudového prostředí:

- Instalace a údržba certifikátů doporučených Poskytovatelem aplikace pro zabezpečení přístupů na servery;
- úpravy výkonnostních parametrů systému a webapps;
- správa souborového systému (filesystem, přístupová práva a zaplněnost datových storů);
- testování změn provedených v OS;
- komunikace a řešení problémů s externí L3 podporou.

Oblast – Provozní služby

2.2 Poskytování správy

Služba je poskytována v cloudovém prostředí SPCSS (Google Cloud platform) a využívá virtuální servery. Služba zahrnuje následující činnosti:

- testování změn provedených v OS;
- administrace operačních systémů;
- aktualizace operačních systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a s ohledem na stabilitu provozu aplikací;
- kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;

- provádění restartů operačních systémů dle požadavků Objednatele
- změny konfigurací OS;
- vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu);
- profylaxe systému dle harmonogramu v měsíčních intervalech;
- součinnosti s případnou instalací a konfigurací nového software;
- instalace a údržba ovladačů a firmware hardwaru.

2.3 Zajišťování provozu bezpečného komunikačního rozhraní

V rámci zajišťování provozu bezpečného komunikačního rozhraní jsou typicky čerpány následující aktivity:

- připojení řešení z datových center SPCSS do internetu. Internetová konektivita je primárně realizována připojením do dvou nezávislých uzlů NIX dvěma nezávislými optickými trasami o kapacitě 10 Gbps a sekundárně připojením dvěma nezávislými linkami 100 Mbps přes ISP;
- připojení řešení z datových center SPCSS do GOVBONE a CMS2. Připojení je zajištěno redundantními propoji v rámci DC SPCSS;
- propojení datových center DC Vápenka a DC Zeleneč – DCI;
- firewall a IPS;
- aplikační firewall a loadbalancer;
- VPN – vzdálené připojení do sítě SPCSS pomocí VPN, a to buď jako site-to-site VPN nebo remote-access VPN. Určeno pro dodavatele pro účely vzdálené správy aplikace.

Součástí výše uvedených položek je následující podpůrná infrastruktura a související služby, které jsou nezbytné pro provoz bezpečného propojení:

- plně redundantní síťová infrastruktura Poskytovatele;
- ochrana proti DoS a DDoS útokům;
- přiřazení a aktualizace bezpečnostních oprávnění uživatelům a zařízením v síti;
- aktualizace a opravy prvků síťové infrastruktury;
- vyhodnocování a optimalizace výkonu sítě a síťových prvků;
- zajištění dokumentace poskytovaných služeb a jejich technického nastavení pro potřeby Objednatele v takovém rozsahu, aby Objednatel byl schopen dokumentovat správu a provoz aplikační vrstvy ve všech provozních stavech podporovaných aplikací;
- řízení provozu a dohled nad kvalitou poskytované Služby;

2.4 Řízení provozu a dohledu nad kvalitou poskytované služby

Řízení provozu vychází z požadavků příslušných standardů ITIL a norem ČSN ISO/IEC 20000.

2.4.1 Řízení provozu Systému zahrnuje zejména:

- koordinaci provozu HW a SW;
- řízení v oblasti rizik a kvality;
- řízení komunikace mezi stranami, které se účastní poskytování služby;
- účastníky poskytování služby;
- koordinaci změnových řízení v rámci poskytování služby;
- personální zajištění řízení provozu služby zahrnuje obsazení role vedoucího provozu služby.

2.4.2 Podpora poskytování služby prostřednictvím SW nástrojů SPCSS zahrnuje zejména:

- poskytování informací pro posouzení postupu řešení nedostupnosti a závad Služby;
- procesní řízení získaných informací;
- SW a personální zajištění.

2.4.3 Dohled nad kvalitou poskytované služby zahrnuje zejména:

- trvalý provozní a bezpečnostní dohled;
- vyhodnocování SLA specifikované v Katalogovém listu.

3 KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

3.1 Požadovaná měsíční dostupnost oblastí služby

Prostředí	Dostupnost oblastí služby	
	Poskytování výpočetního výkonu	Zajišťování provozu bezpečného komunikačního rozhraní
Produktivní	99,5 %	99,5 %
Pre-produktivní	95,0 %	95,0 %
Testovací	95,0 %	95,0 %

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 \times \frac{T - N}{T}$$

kde

D je dostupnost [%] v daném období.

T vyjadřuje fond provozní doby služby v daném období.

N vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky schválené mimořádné odstávky.

Servisní okna poskytované služby jsou ve čtvrtek od 20:00 do 6:00, a pokud budou mít činnosti v servisním okně dopad do dostupnosti, bude Poskytovatel žádat o jejich schválení formou mimořádné odstávky.

3.2 Požadované lhůty pro obnovení služby

Prostředí	Lhůta pro obnovení služby v hodinách v běžné provozní době		
	Incident kategorie A	Incident kategorie B	Incident kategorie C
Produktivní	4	6	24
Pre-produktivní	24	72	168
Testovací	24	72	168

Kategorizace incidentů:

Incident kategorie A	Služba není použitelná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje jeho užívání většině nebo všem jejím uživatelům. Tento stav kritickým způsobem ohrožuje běžný provoz Objednatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody, a při tom neexistuje náhradní způsob zajištění poskytování služeb tohoto systému.
Incident kategorie B	Služba, je ve svých funkcích degradována tak, že tento stav zásadně omezuje běžný provoz Objednatele.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

4 CENA SLUŽBY

Rozdělení služby dle odst. 2 tohoto katalogového listu	Měsíční cena v Kč (MF/02)		
	bez DPH	DPH	s DPH
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu (Cloudová služba)	Cena za Cloudové služby je stanovena dle skutečně čerpaného plnění za jeden kalendářní měsíc poskytování Cloudových služeb. Vyúčtování Cloudové služby bude provedeno dle mechanismu, který je stanoven v tomto katalogovém listu.		
2.1 Poskytování výpočetního výkonu (Infra služba)	10 439,00	2 192,19	12 631,19
2.2 Poskytování správy (Provozní služba)	61 446,00	12 903,66	74 349,66
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	49 597,00	10 415,37	60 012,37
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	120 186,00	25 239,06	145 425,06
Celková měsíční cena	**241 668,00**	**50 750,28**	**292 418,28**

Cena je stanovena dle skutečného čerpání Cloudových služeb, tj. jednotek Google Cloud platform pro jednotlivé Informační Systémy, resp. jejich jednotlivá prostředí.

Poskytovatel bude fakturovat skutečnou cenu za spotřebované jednotky dle faktury dodavatele. Přílohou faktury je i kopie faktury dodavatele.

5 SMLUVNÍ POKUTY ZA NESPLNĚNÍ KVALITATIVNÍCH PARAMETRŮ POSKYTOVÁNÍ SLUŽBY

Za porušení kvalitativních parametrů, tzn. za nedodržení dostupnosti služby dle pododst. 3.1 a nedodržení požadované lhůty pro obnovení služby dle pododst. 3.2, je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu vypočítanou za jednotlivé oblasti služby dle odst. 2 tohoto katalogového listu.

Název parametru	Smluvní pokuta za porušení parametru služby v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Max. výše smluvní pokuty v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Způsob výpočtu
Dostupnost oblasti Služby	1	40	za každých započatých 15 minut nad povolený limit nedostupnosti nebo doby vyřešení incidentu
Doba vyřešení incidentu kategorie A	1	40	
Doba vyřešení incidentu kategorie B	0,5	15	
Doba vyřešení incidentu kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období.

Výše smluvní pokuty se při nedodržení dostupnosti konkrétního prostředí nebo nedodržení doby vyřešení incidentu vypočítá jako procento z celkové měsíční ceny služby dle tabulky v odst. 4. tohoto katalogového listu.

MF/03	Provoz informačních portálů

1 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba bude poskytována v provozní době 24x7 hodin.

Celková doba je rozdělena na dvě části, běžnou provozní dobu (v kalendářních dnech od 6:00 hod do 20:00 hod) a rozšířenou provozní dobu (v kalendářních dnech od 20:00 hod do 6:00 hod).

2 POPIS ROZSAHU SLUŽBY

Obsahem Služby je zajištění bezpečného produkčního prostředí Informačních portálů MF ČR a jeho spolehlivého provozu pomocí cloudových služeb SPCSS (MS Azure).

<table>
<tr><th colspan="4">Prostředí pro Službu provoz informačních portálů – Platforma x64</th></tr>
<tr><th>Prostředí</th><th>CPU</th><th>RAM (GB)</th><th></th></tr>
<tr><td>Produktivní</td><td colspan="3" rowspan="2">Celkový poskytovaný rozsah pro obě prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č.4 Smlouvy).
Výkaz alokace výpočetního výkonu bude Poskytovatel předkládat Objednateli na vyžádání.</td></tr>
<tr><td>Testovací</td></tr>
<tr><td>Celkový rezervovaný výkon</td><td colspan="3">4 000 kreditů</td></tr>
</table>

Oblast – cloudové služby

2.1 Poskytování výpočetního výkonu

Služba je realizována prostřednictvím cloudových služeb SPCSS (MS Azure). Architektura prostředí je designována, co se výkonu týká, jako dynamicky škálovatelná a maximálně využívá webapp cloudových služeb SPCSS (MS AZURE).

Poskytování správy cloudového prostředí:

- Instalace a údržba certifikátů doporučených Poskytovatelem aplikace pro zabezpečení přístupů na servery;
- úpravy výkonnostních parametrů systému a webapps;
- správa souborového systému (filesystem, přístupová práva a zaplněnost datových storů);
- testování změn provedených v OS;
- komunikace a řešení problémů s externí L3 podporou;
- monitorovací a analytický nástroj Matomo.

Oblast – Provozní služby

2.2 Poskytování správy

Služba je poskytována v cloudovém prostředí SPCSS (MS AZURE) využívá služeb webapps a virtuální servery, které běží na následujících operačních systémech MS Windows (MS Windows Server 2016 a vyšší):

- instalace a údržba certifikátů doporučených Poskytovatelem aplikace pro zabezpečení přístupů na servery;
- testování změn provedených v OS;
- administrace operačních systémů;
- aktualizace operačních systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a s ohledem na stabilitu provozu aplikací;
- kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;
- provádění restartů operačních systémů dle požadavků Objednatele;
- změny konfigurací OS;
- vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu);
- profylaxe systému dle harmonogramu v měsíčních intervalech;
- součinnosti s případnou instalací a konfigurací nového software;
- instalace a údržba ovladačů a firmware hardwaru.

2.3 Zajišťování provozu bezpečného komunikačního rozhraní

V rámci zajišťování provozu bezpečného komunikačního rozhraní jsou typicky čerpány následující aktivity:

- připojení řešení z datových center SPCSS včetně cloud operátorů do internetu;
- připojení řešení z datových center SPCSS do GOVBONE a CMS2. Připojení je zajištěno redundantními propoji v rámci DC SPCSS;
- firewall a IPS;
- aplikační firewall a loadbalancer;
- VPN – vzdálené připojení do sítě SPCSS pomocí VPN, a to buď jako site-to-site VPN nebo remote-access VPN. Určeno pro dodavatele pro účely vzdálené správy aplikace.

Součástí výše uvedených položek je následující podpůrná infrastruktura a související služby, které jsou nezbytné pro provoz bezpečného propojení:

- plně redundantní síťová infrastruktura Poskytovatele;
- ochrana proti DoS a DDoS útokům;
- přiřazení a aktualizace bezpečnostních oprávnění uživatelům a zařízením v síti;
- aktualizace a opravy prvků síťové infrastruktury.

2.4 Řízení provozu a dohled na kvalitou poskytovaných služeb

2.4.1 Oblast služby zahrnuje zejména:

- koordinaci provozu HW a SW;
- řízení v oblasti rizik a kvality;
- řízení komunikace stran, které se účastní poskytování služby;
- koordinaci změnových řízení v rámci poskytování služby;
- personální zajištění řízení provozu služby zahrnuje obsazení role vedoucího provozu služby.

2.4.2 Podpora poskytování služby prostřednictvím SW nástrojů SPCSS zahrnuje zejména:

- poskytování informací pro posouzení postupu řešení nedostupnosti a závad služby;
- procesní řízení získaných informací;
- SW a personální zajištění.

2.4.3 Dohled nad kvalitou poskytované služby zahrnuje zejména:

- trvalý provozní a bezpečnostní dohled;
- vyhodnocování SLA specifikovaná v Katalogovém listu.

Provoz informačních portálů musí splňovat veškeré požadavky na Významný informační systém dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), včetně dalších požadavků prováděcích předpisů a nařízení, zejména Směrnice SŘBI MF. SPCSS je ve vztahu k MF významným dodavatelem a provozovatelem informačních portálů.

Bezpečnost a dohledy na úrovni infrastruktury obsahuje bezpečnostní a provozní dohled na úrovni odpovídající charakteru části služby:

- poskytování výpočetního výkonu;
- poskytování správy operačních systémů;
- zajišťování provozu bezpečného komunikačního rozhraní.

Pravidelným měsíčním výstupem bezpečnostního dohledu je zpracování Zprávy o stavu bezpečnosti infrastruktury, která je součástí Zprávy a obsahuje také informace o bezpečnostním monitoringu služby služby MF/09 – Open data podle této přílohy.

Poskytovatel se zavazuje tímto plnit povinnosti, které vychází ze shora uvedené legislativy.

Poskytovatel je povinen při poskytování infrastrukturních služeb plně implementovat a provádět ustanovení ZoKB a VoKB, zejména:

- zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti Významného informačního systému a vést o nich bezpečnostní dokumentaci;
- provádět opatření dle § 11 ZoKB;
- vést veškeré provozní a bezpečnostní záznamy infrastruktury, realizovat organizační a technická opatření požadovaná MF ke sběru a vyhodnocování záznamů dle vyhlášky č. 82/2018 Sb. vlastními prostředky;
- informovat Manažera kybernetické bezpečnosti MF o zranitelnostech, hrozbách a rizicích a jejich zvládání a pravidelných revizí;
- hlásit Manažeru kybernetické bezpečnosti o bezpečnostních hlášeních, kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech bez zbytečného odkladu;
- hlásit kybernetické bezpečnostní incidenty na Národní úřad pro kybernetickou a informační bezpečnost formou požadovanou VoKB a Manažera kybernetické bezpečnosti MF informovat a hlášení KBI na NÚKIB bez zbytečného odkladu o kybernetických bezpečnostních incidentech, a to bezodkladně po jejich detekci;
- realizovat bezpečnostní opatření ke zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů po konzultaci s Manažerem kybernetické bezpečnosti MF;
- umožnit přístup pro určené osoby Objednatele k řešení tiketů do systému Service Desk Poskytovatele, Manažerovi kybernetické bezpečnosti MF nebo dalším určeným osobám vzdálený přístup k záznamům týkajícím se IISSP v nástroji SIEM;
- nakládat s daty, která budou smazána v souladu s jejich účelem a dodržovat pravidla pro likvidaci dat;
- v rozsahu služby dodržovat Směrnice MF a realizovat bezpečnostní opatření ve formě organizačních a technických opatření i na SPCSS;
- komunikovat s MF kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty v rozsahu poskytovaných služeb nebo rozsahu, který by ovlivňoval poskytované služby;
- řídit bezpečnostní rizika;
- řídit kontinuitu provozu;
- předávat předem dohodnutou formou data, provozní údaje a informace vyžádané Objednatelem;

- řídit změny.

3 KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

3.1 Požadovaná měsíční dostupnost prostředí

Prostředí	Dostupnost oblastí služby	
	Poskytování výpočetního výkonu	**Zajišťování provozu bezpečného komunikačního rozhraní**
Produktivní	99,5 %	99,5 %
Testovací	95,0 %	95,0 %

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 \times \frac{T - N}{T}$$

kde

D je dostupnost [%] v daném období.

T vyjadřuje fond provozní doby služby v daném období.

N vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky schválené mimořádné odstávky.

Servisní okna poskytované služby jsou ve čtvrtek od 20:00 do 6:00 a pokud budou mít činnosti v servisním okně dopad do dostupnosti, bude Poskytovatel žádat o jejich schválení formou mimořádné odstávky.

3.2 Požadované lhůty pro obnovení služby

Prostředí	Lhůta pro obnovení služby v hodinách v běžné provozní době		
	Incident kategorie A	Incident kategorie B	Incident kategorie C
Produktivní	4	6	24
Testovací	24	72	168

Kategorizace incidentů:

Incident kategorie A	Služba není použitelná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje jeho užívání většině nebo všem jejím uživatelům. Tento stav kritickým způsobem ohrožuje běžný provoz Objednatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody, a při tom neexistuje náhradní způsob zajištění poskytování služeb tohoto systému.
Incident kategorie B	Služba, je ve svých funkcích degradován tak, že tento stav zásadně omezuje běžný provoz Objednatele.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

4 CENA SLUŽBY

Rozdělení služby dle odst. 2 tohoto katalogového listu	Měsíční cena v Kč (MF/03)		
	bez DPH	DPH	s DPH
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu (Cloudová služba)	Cena za Cloudové služby je stanovena dle skutečně čerpaného plnění za jeden kalendářní měsíc poskytování Cloudových služeb. Vyúčtování Cloudové služby bude provedeno dle mechanismu, který je stanoven v tomto katalogovém listu.		
2.1 Poskytování výpočetního výkonu (Infra služba)	19 874,00	4 173,54	24 047,54
2.2 Poskytování správy (Provozní služba)	48 288,00	10 140,48	58 428,48
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	62 836,00	13 195,56	76 031,56
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	106 585,00	22 382,85	128 967,85

Rozdělení služby dle odst. 2 tohoto katalogového listu	Měsíční cena v Kč (MF/03)		
	bez DPH	DPH	s DPH
Měsíční cena v období od 01.04.2025 do 31.03.2028			
Celková měsíční cena	**237 583,00**	**49 892,43**	**287 475,43**

Cena je stanovena dle skutečného čerpání Cloudových služeb, tj. Azure jednotek pro jednotlivé Informační Systémy, resp. jejich jednotlivá prostředí.

Pro účely fakturace Cloudových služeb je stanoveno, že 1 Azure Jednotka = 1 Euro. Kurz Euro dle nákupu Azure Jednotek Poskytovatelem je stanoven na 25,155 Kč/Euro a je pro Objednatele závazný, pokud nebude ze strany Poskytovatele oznámen Objednateli nový kurz Euro za nákup Azure jednotek, a to prostřednictvím příslušného Záznamu. V každém měsíčním Záznamu bude Poskytovatelem uveden kurz Euro, za který byly nakoupeny předmětné Azure jednotky a tento kurz je pro Smluvní strany závazný. Poskytovatel se zavazuje v Záznamu vždy uvést konkrétní den, ke kterému došlo ke změně kurzu Euro. Pro vyloučení pochybností Smluvní strany výslovně uvádějí, že tato změna kurzu není důvodem k uzavření dodatku ke Smlouvě a bude provedena jednostranně ze strany Poskytovatele.

5 SMLUVNÍ POKUTY ZA NESPLNĚNÍ KVALITATIVNÍCH PARAMETRŮ POSKYTOVÁNÍ SLUŽBY

Název parametru	Smluvní pokuta za porušení parametru služby v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Max. výše smluvní pokuty v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Způsob výpočtu
Dostupnost prostředí	1	40	za každých započatých 15 minut nad povolený limit nedostupnosti nebo doby vyřešení incidentu
Doba vyřešení incidentu kategorie A	1	40	
Doba vyřešení incidentu kategorie B	0,5	15	
Doba vyřešení incidentu kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období.

Výše smluvní pokuty se při nedodržení dostupnosti konkrétního prostředí nebo nedodržení doby vyřešení incidentu vypočítá jako procento z celkové měsíční ceny služby dle tabulky v odst. 4 tohoto katalogového listu.

MF/04	Kapacita HSM (Hardware Security Module)

1 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba HSM pro IISSP a resortní PKI podle tohoto katalogového listu bude poskytována v režimu 24x7 hodin. Celková doba je rozdělena na dvě části, běžnou provozní dobu (v kalendářních dnech od 6:00 hod do 20:00 hod) a rozšířenou provozní dobu (v kalendářních dnech od 20:00 hod do 6:00 hod).

2 POPIS ROZSAHU SLUŽBY

Obsahem služby kapacita HSM pro IISSP a resortní PKI je zajištění bezpečného produkčního prostředí subsystému a jeho spolehlivého provozu.

Pro kryptografické operace jsou využity HSM typu Thales nCipher 1500+ nebo novější, s kapacitou až 1260 transakcí za vteřinu při 256bit délce šifrovacího klíče a možného počtu 20 klientských stanic.

Pro šifrovací operaci může být v daném HSM modulu poskytnuta operátorská karta, která umožňuje použít šifrovací klíče uložené na aplikačním serveru Objednatele.

Oblast – Infra služby

2.1 Poskytování výpočetního výkonu

Služba bude realizována prostřednictvím virtuálních serverů, komunikujících s moduly HSM realizující kryptografické operace. Garantované parametry výkonu jsou uvedeny v následující tabulce:

Prostředí pro provoz HSM	
Garantovaný podpisový výkon (tps) RSA pro klíče doporučené NIST	
2048 bit	450
4096 bit	190
Garantovaný podpisový výkon (tps) pro eliptické křivky ECC pro NIST doporučené klíče	
256 bit	1 260
Garantovaný počet přistupujících klientů	5

Oblast – Provozní služby

2.2 Poskytování správy HSM

Služba zahrnuje následující činnosti:

- administrace systémů, tzn. incident management, problem management a change management (vyjma projektových změn);
- aktualizace (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost aplikací;
- kontrola existence bezpečnostních patchů a analýza jejich dopadů na provoz;
- vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu);
- profylaxe systému dle harmonogramu v měsíčních intervalech;
- součinnosti s případnou instalací a konfigurací nového software;
- instalace a údržba certifikátů doporučených dodavatelem aplikace pro zabezpečení přístupů;
- správa lokálních uživatelských účtů;
- úpravy výkonnostních parametrů systému;
- správa souborového systému (filesystem, přístupová práva a zaplněnost);
- součinnost při testech obnovy klíčů.

2.3 Zajišťování provozu bezpečného komunikačního rozhraní

V rámci zajišťování provozu bezpečného komunikačního rozhraní jsou typicky čerpány následující aktivity:

- připojení řešení z datových center SPCSS do GOVBONE a CMS2. Připojení je zajištěno redundantními propoji v rámci DC SPCSS;
- firewall a IPS;
- aplikační firewall a loadbalancer;
- VPN – vzdálené připojení do sítě SPCSS pomocí VPN, a to buď jako site-to-site VPN nebo remote-access VPN. Určeno pro dodavatele pro účely vzdálené správy aplikace.

Součástí výše uvedených položek je následující podpůrná infrastruktura a související služby, které jsou nezbytné pro provoz bezpečného propojení:

- plně redundantní síťová infrastruktura Poskytovatele;
- přiřazení a aktualizace bezpečnostních oprávnění uživatelům a zařízením v síti;
- aktualizace a opravy prvků síťové infrastruktury.

Součástí výše uvedených položek je následující podpůrná infrastruktura a související služby, které jsou nezbytné pro provoz bezpečného propojení:

- plně redundantní síťová infrastruktura Poskytovatele;
- ochrana proti DoS a DDoS útokům;
- přiřazení a aktualizace bezpečnostních oprávnění uživatelům a zařízením v síti;
- aktualizace a opravy prvků síťové infrastruktury;
- vyhodnocování a optimalizace výkonu sítě a síťových prvků;
- zajištění dokumentace poskytovaných služeb a jejich technického nastavení pro potřeby Objednatele v takovém rozsahu, aby Objednatel byl schopen dokumentovat správu a provoz aplikační vrstvy ve všech provozních stavech podporovaných aplikací.
- řízení provozu a dohled nad kvalitou poskytované služby;
- řízení provozu a dohledu nad kvalitou poskytované služby vychází z požadavků příslušných standardů ITIL a norem ČSN ISO/IEC 20000.

2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb

2.4.1 Oblast služby zahrnuje především:

- koordinaci provozu HW a SW;
- řízení v oblasti rizik a kvality;
- řízení komunikace se všemi stranami, které se podílejí na poskytování služby;
- koordinaci změnových řízení v rámci poskytování služby;
- personální zajištění řízení provozu služby zahrnuje obsazení role vedoucího provozu služeb.

2.4.2 Podpora poskytování služby prostřednictvím SW nástrojů SPCSS zahrnuje zejména:

- poskytování informací pro posouzení postupu řešení nedostupnosti a závad služby;
- procesní řízení získaných informací;
- SW a personální zajištění.

2.4.3 Dohled nad kvalitou poskytované služby zahrnuje zejména:

- trvalý provozní a bezpečnostní dohled;
- vyhodnocování SLA specifikované v Katalogovém listu.

2.4.4 Bezpečnost a dohledy na úrovni infrastruktury

Služba obsahuje bezpečnostní a provozní dohled na úrovni odpovídající charakteru části služby:

- poskytování výpočetního výkonu;
- poskytování správy operačních systémů;

- zajišťování provozu bezpečného komunikačního rozhraní.

Služba poskytuje přímou podporu provozu IISSP a musí splňovat veškeré požadavky na informační systém Kritické informační infrastruktury dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), včetně dalších požadavků prováděcích předpisů a nařízení, zejména Směrnice SŘBI MF. SPCSS je ve vztahu k MF významným dodavatelem HSM modulů. Zpráva o stavu bezpečnosti infrastruktury HSM modulů je integrální součástí zprávy ke službě MF/01.

Poskytovatel se zavazuje tímto plnit povinnosti, které vycházejí ze shora uvedené legislativy:

Poskytovatel je povinen při poskytování infrastrukturních služeb plně implementovat a provádět ustanovení ZoKB a VoKB, zejména:

- zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury a vést o nich bezpečnostní dokumentaci;
- provádět opatření dle § 11 ZoKB;
- vést veškeré provozní a bezpečnostní záznamy infrastruktury, realizovat organizační a technická opatření požadovaná MF ke sběru a vyhodnocování záznamů dle vyhlášky č. 82/2 018 Sb. vlastními prostředky;
- informovat Manažera kybernetické bezpečnosti MF o zranitelnostech, hrozbách a rizicích a jejich zvládání a pravidelných revizích;
- hlásit Manažeru kybernetické bezpečnosti MF o bezpečnostních hlášeních, kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech bez zbytečného odkladu;
- hlásit kybernetické bezpečnostní incidenty na Národní úřad pro kybernetickou a informační bezpečnost formou požadovanou VoKB a Manažera kybernetické bezpečnosti MF informovat a hlášení KBI na NÚKIB bez zbytečného odkladu;
- realizovat bezpečnostní opatření ke zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů po konzultaci s Manažera kybernetické bezpečnosti MF;
- umožnit přístup pro určené osoby Objednatele pro řešení tiketů do systému Service Desk Poskytovatele, Manažerovi kybernetické bezpečnosti MF nebo dalším určeným osobám vzdálený přístup k záznamům týkajícím se služby v nástroji SIEM;
- nakládat s daty služby určenými k likvidaci v souladu s jejich účelem a dodržovat pravidla pro likvidaci dat;
- v rozsahu služby dodržovat Směrnice MF a realizovat bezpečnostní opatření ve formě organizačních a technických opatření i na SPCSS;
- komunikovat s MF kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty v rozsahu poskytovaných služeb nebo rozsahu, který by ovlivňoval poskytované služby;
- řídit bezpečnostní rizika služby;
- řídit kontinuitu provozu služby;
- předávat předem dohodnutou formou data, provozní údaje a informace vyžádané Objednatelem;
- řídit změny.

3 KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

3.1 Požadovaná měsíční dostupnost oblastí služby

Prostředí	Dostupnost oblastí služby

	Poskytování výpočetního výkonu	Zajišťování provozu bezpečného komunikačního rozhraní
Produktivní	99,5 %	99,5 %
Pre-produktivní	95,0 %	95,0 %
Vývojové	95,0 %	95,0 %
Testovací	95,0 %	95,0 %

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 \times \frac{T - N}{T}$$

kde

D je dostupnost [%] v daném období.

T vyjadřuje fond provozní doby služby v daném období.

N vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky schválené mimořádné odstávky.

Servisní okna poskytované služby jsou ve čtvrtek od 20:00 do 6:00 a pokud budou mít činnosti v servisním okně dopad do dostupnosti, bude Poskytovatel žádat o jejich schválení formou mimořádné odstávky.

3.2 Požadované lhůty pro obnovení služby

Prostředí	Lhůta pro obnovení služby v hodinách v běžné provozní době		
	Incident kategorie A	Incident kategorie B	Incident kategorie C
Produktivní	4	6	24
Pre-produktivní	24	72	168
Vývojové	24	72	168
Testovací	24	72	168

Kategorizace incidentů:

Incident kategorie A	Služba není použitelná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje jeho užívání většině nebo všem jejím uživatelům. Tento stav kritickým způsobem ohrožuje běžný provoz Objednatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody, a při tom neexistuje náhradní způsob zajištění poskytování služeb tohoto systému.
Incident kategorie B	Služba, je ve svých funkcích degradován tak, že tento stav zásadně omezuje běžný provoz Objednatele.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

3.3 Požadované lhůty pro obnovení služby pro vybrané komponenty

Lhůty pro obnovení služby v Produkčním prostředí provozovaném v době konání plánovaného a odsouhlaseného Disaster Recovery testu (komponenty Služby 2.1 Poskytování

výpočetního výkonu a 2.3 zajišťování provozu bezpečného komunikačního rozhraní) jsou stejné jako v testovacím prostředí, tedy:

Incident kategorie A	24 hodin v běžné provozní době
Incident kategorie B	72 hodin v běžné provozní době
Incident kategorie C	168 hodin v běžné provozní době

4 CENA SLUŽBY

Rozdělení služby dle odst. 2 tohoto katalogového listu	Měsíční cena v Kč (MF/04)		
	bez DPH	DPH	s DPH
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu (Infra služba)	467 775,00	98 232,75	566 007,75
2.2 Poskytování správy HSM (Provozní služba)	49 324,00	10 358,04	59 682,04
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	40 053,00	8 411,13	48 464,13
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	27 283,00	5 729,43	33 012,43
Celková měsíční cena	**584 435,00**	**122 731,35**	**707 166,35**

5 SMLUVNÍ POKUTY ZA NESPLNĚNÍ KVALITATIVNÍCH PARAMETRŮ POSKYTOVÁNÍ SLUŽBY

Za porušení kvalitativních parametrů, nedodržení požadované měsíční dostupnosti dle pododst. 3.1 a lhůty pro obnovení služby dle pododst. 3.2, je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu vystavenou za jednotlivé oblasti služby dle odst. 2 tohoto katalogového listu.

Název parametru	Smluvní pokuta za porušení parametru služby v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Max. výše smluvní pokuty v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Způsob výpočtu
Dostupnost oblasti Služby	1	40	za každých započatých 15 minut nad povolený limit nedostupnosti nebo doby vyřešení incidentu
Doba vyřešení incidentu kategorie A	1	40	
Doba vyřešení incidentu kategorie B	0,5	15	
Doba vyřešení incidentu kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období.

Výše smluvní pokuty se při nedodržení dostupnosti konkrétního prostředí nebo nedodržení doby vyřešení incidentu vypočítá jako procento z celkové měsíční ceny služby dle tabulky v odst. 4 tohoto katalogového listu.

MF/05	Zajištění a provoz produkčního prostředí IS APAO

1 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba bude poskytována pro produktivní prostředí IS APAO v režimu 24x7 hodin.

Celková doba je rozdělena na dvě části, běžnou provozní dobu (v kalendářních dnech od 6:00 hod do 20:00 hod) a rozšířenou provozní dobu (v kalendářních dnech od 20:00 hod do 6:00 hod).

Testovací/referenční prostředí bude poskytováno v režimu 8x5 hodin ve zkrácené provozní době, tj. v pracovních dnech od 8:00 do 16:00 hod. Pro účely vyhodnocení SLA „Lhůta pro obnovení služby v běžné provozní době v hodinách" je u testovacího/referenčního prostředí běžná provozní doba od 8:00 do 16:00 hod.

Služba bude poskytovaná v rámci On-premise datových center SPCSS.

2 POPIS ROZSAHU SLUŽBY

Obsahem služby Zajištění a provoz produkčního prostředí pro IS APAO v režimu podle odst. 1 tohoto Katalogového listu je zajištění bezpečného a spolehlivého provozu tohoto prostředí. V termínu zahájení poskytování služby Zajištění a provoz prostředí pro IS APAO podle tohoto katalogového listu má MF k dispozici HW infrastrukturu uvedeného prostředí pro provoz IS APAO.

Oblast – Infra služby

2.1 Poskytování výpočetního výkonu

Služba bude realizována prostřednictvím zdrojů výpočetního výkonu x64 – VMWare, které mají dostatečný výpočetní výkon pro provozování IS APAO a požadovanou dostupnost.

Architektura infrastruktury umožňuje pro všechny prvky (servery, storage i komunikace) standardní škálování vertikálně i horizontálně s minimálním dopadem na provoz.

2.1.1 Výpočetní výkon na platformě x64

Výpočetní výkon na platformě x64 – VMWare je poskytován na technologiích Intel Xeon E5-2630 v4 a vyšší skrze optimalizované virtuální servery s operačními systémy Windows nebo Linux.

V ceně služby je zahrnuto i umístění v datovém centru včetně racku a energie.

Alokace je realizována prostředky virtualizační platformy a je v odpovědnosti Poskytovatele.

Prostředí pro provoz IS APAO – Platforma x64			
Prostředí	**CPU**	**RAM (GB)**	**Diskový prostor (GB)**
Produktivní	Celkový poskytovaný výkon pro jednotlivá prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č.4 Smlouvy).		
Testovací/Referenční			
Celkový rezervovaný výkon	**48**	**128**	**21 000**

2.1.2 Poskytování zálohovacích kapacit

Způsob realizace zálohování respektuje požadavky na dostupnost, výkonnost a umožňuje využít možnosti HW a technologií produkčního prostředí IS APAO, zejména diskových polí a páskových knihoven. Zálohovací systém realizuje zálohování stanoveným způsobem a režimem nutným k zajištění SLA. Standardem je zálohování operačních systémů, vybraných souborových systémů a databází.

Oblast – Provozní služby

2.2 Poskytování správy, servisní podpory SW a údržby HW

2.2.1 Poskytování správy operačních systémů

Služba je poskytována na následujících operačních systémech:

- MS Windows: MS Windows Server Datacenter 2016 a vyšší;
- RedHat 8.1 a vyšší.

Předpokladem služby pro licencované operační systémy je zajištění licence a maintenance OS.

Součástí služby není implementace a správa aplikačních komponent operačních systémů, respektive aplikačního SW přibaleného k základnímu OS, jako jsou například web servery, aplikační servery, middleware, nebo adresářové služby pro účely správy aplikačních uživatelů.

Služba zahrnuje následující činnosti:

- administrace operačních systémů, tzn. incident management, problem management a change management (vyjma změn aplikačních komponent – viz výše);
- aktualizace operačních systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost aplikací;
- kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;
- provádění restartů operačních systémů dle požadavků Objednatele;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- součinnosti s případnou instalací a konfigurací nového software;

- instalace a údržba certifikátů doporučených dodavatelem aplikace pro zabezpečení přístupů na servery;
- úpravy výkonnostních parametrů systému;
- správa souborového systému (filesystem, přístupová práva a zaplněnost);
- testování změn provedených v OS;
- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);
- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele probíhá formou nástrojů typu sudo nebo jsou řízeny pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;
- Poskytovatel instaluje vždy minimální výchozí instalaci operačního systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace (balíčky, filesystemy, úpravy v konfiguračních souborech).

2.2.2 Poskytování správy databází

Služba je poskytována na následujících verzích databázového systému:

- PostgreSQL 14.x a vyšší.

Předpokladem služby pro licencované databázové systémy je zajištění licence a její maintenance.

Služba zahrnuje následující činnosti:

- administrace databázových systémů, tzn. incident management, problem management a change management;
- aktualizace databázových systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost databází;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- úpravy výkonnostních parametrů databáze;
- testování změn provedených v databázi;
- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);
- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele je řízeno pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;
- Poskytovatel instaluje vždy minimální výchozí instalaci databázového systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace.

2.3 Zajišťování provozu bezpečného komunikačního rozhraní

V rámci zajišťování provozu bezpečného komunikačního rozhraní jsou typicky čerpány následující aktivity:

- připojení řešení z datových center SPCSS do internetu. Internetová konektivita je primárně realizována připojením do dvou nezávislých uzlů NIX dvěma nezávislými optickými trasami o kapacitě 10 Gbps a sekundárně připojením dvěma nezávislými linkami 100 Mbps přes ISP;
- připojení řešení z datových center SPCSS do GOVBONE. Připojení je zajištěno redundantními propoji v rámci DC SPCSS;
- propojení datových center DC Vápenka a DC Zeleneč – DCI;
- firewall a IPS;
- aplikační firewall a loadbalancer F5;
- VPN – vzdálené připojení do sítě SPCSS pomocí VPN, a to buď jako site-to-site VPN nebo remote-access VPN. Určeno pro dodavatele pro účely vzdálené správy aplikace.

Součástí výše uvedených položek je následující podpůrná infrastruktura a související služby, které jsou nezbytné pro provoz bezpečného propojení:

- plně redundantní síťová infrastruktura Poskytovatele;
- ochrana proti DoS a DDoS útokům;
- přiřazení a aktualizace bezpečnostních oprávnění uživatelům a zařízením v síti;
- aktualizace a opravy prvků síťové infrastruktury;
- vyhodnocování a optimalizace výkonu sítě a síťových prvků;
- zajištění dokumentace poskytovaných služeb a jejich technického nastavení pro potřeby Objednatele v takovém rozsahu, aby Objednatel byl schopen dokumentovat správu a provoz aplikační vrstvy ve všech provozních stavech podporovaných aplikací;
- řízení provozu a dohled nad kvalitou poskytované služby;
- řízení provozu a dohledu nad kvalitou poskytované služby vychází z požadavků příslušných standardů ITIL a norem ČSN ISO/IEC 20000.

2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb

2.4.1 Řízení provozu Systému zahrnuje zejména:

- koordinaci provozu HW a SW;
- řízení v oblasti rizik a kvality;
- řízení komunikace mezi dodavatelem aplikace a poskytovatelem;
- koordinaci změnových řízení v rámci poskytování služby.

2.4.2 Podpora poskytování služby prostřednictvím SW nástrojů SPCSS zahrnuje zejména:

- poskytování informací pro posouzení postupu řešení nedostupnosti a závad služby;
- procesní řízení získaných informací;
- SW a personální zajištění.

2.4.3 Dohled nad kvalitou poskytované služby zahrnuje zejména:

- trvalý provozní a bezpečnostní dohled;
- vyhodnocování SLA specifikované v Katalogovém listu.

Infrastruktura SPCSS splňuje veškeré požadavky na provozování IS APAO který je klasifikovaný jako Významný informační systém dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), včetně dalších požadavků prováděcích předpisů a nařízení. SPCSS je ve vztahu k MF významným dodavatelem a provozovatelem technických prostředků IS APAO.

Bezpečnost a dohledy na úrovni infrastruktury obsahuje bezpečnostní a provozní dohled na úrovni odpovídající charakteru části služby:

- poskytování výpočetního výkonu;
- poskytování správy operačních systémů;
- poskytování správy databází;
- zajišťování provozu bezpečného komunikačního rozhraní.

Pravidelným měsíčním výstupem bezpečnostního dohledu je zpracování Zprávy o stavu bezpečnosti infrastruktury, která je součástí Zprávy.

Poskytovatel se zavazuje tímto plnit povinnosti, které vychází ze shora uvedené legislativy.

Poskytovatel je povinen při poskytování infrastrukturních služeb plně implementovat a provádět ustanovení ZoKB a VoKB, zejména:

- zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti Významného informačního systému a vést o nich bezpečnostní dokumentaci;
- provádět opatření dle § 11 ZoKB;
- vést veškeré provozní a bezpečnostní záznamy infrastruktury, realizovat organizační a technická opatření požadovaná MF ke sběru a vyhodnocování záznamů dle vyhlášky č. 82/2018 Sb. vlastními prostředky;
- informovat Manažera kybernetické bezpečnosti MF o zranitelnostech, hrozbách a rizicích a jejich zvládání a pravidelných revizí;
- hlásit Manažeru kybernetické bezpečnosti MF o bezpečnostních hlášeních, kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech bez zbytečného odkladu;
- hlásit kybernetické bezpečnostní incidenty na Národní úřad pro kybernetickou a informační bezpečnost formou požadovanou VoKB a Manažera kybernetické bezpečnosti MF informovat a hlášení KBI na NÚKIB bez zbytečného odkladu o kybernetických bezpečnostních incidentech, a to bezodkladně po jejich detekci;
- realizovat bezpečnostní opatření ke zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů po konzultaci s Manažerem kybernetické bezpečnosti MF;
- umožnit přístup pro určené osoby Objednatele k řešení tiketů do systému Service Desk Poskytovatele, Manažerovi kybernetické bezpečnosti MF nebo dalším určeným osobám vzdálený přístup k záznamům týkajícím se IS APAO v nástroji SIEM;
- komunikovat s MF kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty v rozsahu poskytovaných služeb nebo rozsahu, který by ovlivňoval poskytované služby;
- řídit bezpečnostní rizika IS APAO;
- řídit kontinuitu provozu IS APAO;
- předávat předem dohodnutou formou data, provozní údaje a informace vyžádané Objednatelem.

3 KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

3.1 Požadovaná měsíční dostupnost oblastí služby

Prostředí	Dostupnost oblastí služby	
	Poskytování výpočetního výkonu a zálohovacích kapacit	**Zajišťování provozu bezpečného komunikačního rozhraní**
Produktivní	99,5 %	99,5 %
Testovací/ Referenční	95,0 %	95,0 %

Nedostupnost služby způsobená hardwarovou nebo jinou technickou závadou infrastruktury některého z prostředí pro provoz IS APAO se počítá od okamžiku zahájení nedostupnosti IS APAO pro koncové uživatele do okamžiku odstranění této závady. V případě,

že není možné prokazatelně zjistit okamžik zahájení nedostupnosti IS APAO pro koncové uživatele, počítá se nedostupnost služby od doby jejího nahlášení do Service Desku SPCSS.

Nedostupnost služby způsobená softwarovou závadou infrastruktury IS APAO (nastavení systému, pravidla a prostupy firewalu, apod.) se počítá od okamžiku nahlášení nedostupnosti IS APAO pro koncové uživatele do okamžiku odstranění této závady.

Za **nahlášení nedostupnosti služby** se považuje založení odpovídajícího servisního hlášení v aplikaci **Service Desk SPCSS** (servicedesk.spcss.cz).

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 \times \frac{T - N}{T}$$

kde

- D je měsíční dostupnost [%] v daném období.
- T vyjadřuje fond provozní doby služby v daném období.
- N vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky schválené mimořádné odstávky.

Servisní okna poskytované služby jsou ve čtvrtek od 20:00 do 6:00 a pokud budou mít činnosti v servisním okně dopad do dostupnosti, bude Poskytovatel žádat o jejich schválení formou mimořádné odstávky.

3.2 Požadované lhůty pro obnovení služby

Prostředí	Lhůta pro obnovení služby v běžné provozní době v hodinách		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Produktivní	4	6	24
Testovací/Referenční	24	72	168

Kategorizace incidentů:

Incident kategorie A	Služba není použitelná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje jeho užívání většině nebo všem jejím uživatelům. Tento stav kritickým způsobem ohrožuje běžný provoz Objednatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody, a při tom neexistuje náhradní způsob zajištění poskytování služeb tohoto systému.
Incident kategorie B	Služba, je ve svých funkcích degradován tak, že tento stav zásadně omezuje běžný provoz Objednatele.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

3.3 Požadované lhůty pro obnovení služby pro vybrané komponenty

Lhůty pro obnovení služby v produktivním prostředí provozovaném v době konání plánovaného a odsouhlaseného Disaster Recovery testu (komponenty služby 2.1 Poskytování výpočetního výkonu a zálohování a 2.3 zajišťování provozu bezpečného komunikačního rozhraní) jsou stejné jako v testovacím prostředí, tedy:

Prostředí	Lhůta pro obnovení služby v běžné provozní době v době konání plánovaného a odsouhlaseného Disaster Recovery testu		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Produktivní	24	72	168

4 CENA SLUŽBY

Rozdělení služby dle odst. 2 tohoto katalogového listu	Měsíční cena v Kč (MF/05)		
	bez DPH	**DPH**	**s DPH**
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	70 191,00	14 740,11	84 931,11
2.2 Poskytování správy, servisní podpory SW a údržby HW (Provozní služba)	55 830,00	11 724,30	67 554,30
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	261 829,00	54 984,09	316 813,09
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	92 322,00	19 387,62	111 709,62
Celková měsíční cena	**480 172,00**	**100 836,12**	**581 008,12**

5 SMLUVNÍ POKUTY ZA NESPLNĚNÍ KVALITATIVNÍCH PARAMETRŮ POSKYTOVÁNÍ SLUŽBY

Za porušení kvalitativních parametrů, nedodržení dostupnosti služby dle pododst. 3.1 a nedodržení požadované lhůty pro obnovení služby dle pododst. 3.2 a pododst. 3.3, je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu vypočítanou za jednotlivé oblasti služby dle odst. 2 tohoto katalogového listu.

Název parametru	Smluvní pokuta za porušení parametru služby v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Max. výše smluvní pokuty v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Způsob výpočtu
Dostupnost oblasti Služby	1	40	za každých započatých 15 minut nad povolený limit nedostupnosti nebo doby vyřešení incidentu
Doba vyřešení incidentu kategorie A	1	40	
Doba vyřešení incidentu kategorie B	0,5	15	

Doba vyřešení incidentu kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období.

Výše smluvní pokuty se při nedodržení dostupnosti konkrétního prostředí nebo nedodržení doby vyřešení incidentu vypočítá jako procento z celkové měsíční ceny služby dle tabulky v odst. 4 tohoto katalogového listu.

MF/06	Zajištění a provoz produkčního prostředí AISG

1 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba bude poskytována v režimu 24x7 hodin.

Provozní doba pro účely měření SLA pro produktivní prostředí DaS a ELK je v režimu 24x7 hodin. Běžná provozní doba pro účely měření SLA pro produktivní prostředí AM je v kalendářních dnech od 6:00 hod do 20:00 hod.

Testovací prostředí, vývojové prostředí a preprodukční/playground prostředí bude poskytováno pouze v režimu 8x5 hodin ve zkrácené provozní době, tj. v pracovních dnech od 8:00 hod do 16:00 hod.

Služba se skládá z následujících prostředí:

- AISG Dozorová a Správní (DaS):
  - Produktivní prostředí;
  - Preprodukční/Playground prostředí;
  - Testovací prostředí.
- AISG Analytický modul (AM):
  - Produktivní prostředí;
  - Testovací prostředí;
  - Playground prostředí;
  - Vývojové prostředí (platforma Power).
- AISG ELK:
  - Produktivní prostředí;
  - Testovací/Vývojové prostředí.

2 POPIS ROZSAHU SLUŽBY

Obsahem služby Zajištění a provoz produkčního prostředí AISG v režimu podle odst. 1 tohoto Katalogového listu je zajištění bezpečného produkčního prostředí AISG a jeho spolehlivého provozu. V termínu zahájení poskytování služby Provoz AISG podle tohoto katalogového listu má MF k dispozici HW infrastrukturu produkčního prostředí pro provoz AISG, která je popsána v jednotlivých oblastech služby.

Oblast – Infra služba

2.1 Poskytování výpočetního výkonu a zálohovacích kapacit

Infra služba bude realizována prostřednictvím virtuálních serverů, které mají dostatečný výpočetní výkon pro AISG a požadovanou dostupnost napříč několika platformami, které jsou provozovány v rámci on-premise datových center SPCSS.

2.1.1 Výpočetní výkon na platformě Power

Výpočetní výkon na RISC platformě Power je poskytován na technologii platformy Power8 a vyšší.

V každém datovém centru jsou umístěny servery pSeries. Jednotlivé servery mají minimálně 2 CPU sockety.

Platforma výpočetního výkonu nemá interní disky, je připojena ke službám poskytování diskových prostorů (definice služeb poskytování diskového prostoru STOR1). Konektivita k diskovému úložišti je zajištěna pomocí redundantního FibreChannel (FC) propojení.

V ceně služby je zahrnuto i umístění v datovém centru včetně racku a energie.

2.1.2 Výpočetní výkon na platformě x64 VMWare

Výpočetní výkon na platformě x64 je poskytován na technologiích Intel Xeon E5-2630 v4 a vyšší skrze optimalizované virtuální servery s operačními systémy Windows nebo Linux.

V ceně služby je zahrnuto i umístění v datovém centru včetně racku a energie.

Alokace je realizována prostředky virtualizační platformy a je v odpovědnosti Poskytovatele infrastruktury.

2.1.3 Výpočetní výkon na platformě x64 AzureStack

Výpočetní výkon na platformě x64 AzureStack je poskytován v rámci obou datových center SPCSS, na technologiích Intel® Xeon® Gold 6248 a vyšší skrze optimalizované virtuální servery Cisco UCS C2420 M5. V ceně služby je zahrnuto i umístění v datovém centru včetně racku a energie.

Alokace výpočetního výkonu je realizována prostředky virtualizační platformy a je v odpovědnosti Poskytovatele infrastruktury.

2.1.4 Celkové výkonnostní parametry všech prostředí on-premise AISG jsou uvedeny v následujících tabulkách:

<table>
<tr><th colspan="4">Prostředí pro provoz DaS – Platforma x64 VMWare</th></tr>
<tr><th>Prostředí</th><th>vCPU</th><th>vRAM</th><th>STORAGE (GB)</th></tr>
<tr><td>Produktivní prostředí</td><td colspan="3" rowspan="3">Celkový poskytovaný výkon pro jednotlivá prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy).</td></tr>
<tr><td>Preprodukční/Playground prostředí*)</td></tr>
<tr><td>Testovací prostředí</td></tr>
<tr><td>Celkový rezervovaný výkon</td><td>254</td><td>644</td><td>26 371</td></tr>
<tr><td>Poznámka*)</td><td colspan="3">Playground a preprodukční prostředí sdílí stejnou infrastrukturu.</td></tr>
</table>

Prostředí pro provoz AM – Platforma x64 VMWare			
Prostředí	**vCPU**	**vRAM**	**STORAGE (GB)**
Produktivní prostředí	Celkový poskytovaný výkon pro jednotlivá prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy).		
Testovací prostředí			
Playground prostředí			
Celkový rezervovaný výkon	**84**	**248**	**16 280**

Prostředí pro provoz AM – Platforma Power			
Prostředí	**vCPU**	**vRAM**	**STORAGE (GB)**
Produktivní prostředí	Celkový poskytovaný výkon pro jednotlivá prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy).		
Testovací prostředí			
Playground prostředí			
Vývojové (development) prostředí			
Celkový rezervovaný výkon	**35**	**1 314**	**929 758**

Prostředí pro provoz ELK – Platforma x64 AzureStack		
Prostředí	**vCPU LIN**	**vRAM (GB)**
Produktivní prostředí	Celkový rozsah pro všechna prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy).	
Testovací prostředí/Vývojové prostředí*)		
Celkový rezervovaný výkon	**96**	**336**
Poznámka*)	V rámci testovacího prostředí je provozováno i prostředí vývojové.	

2.1.5 Poskytování diskových a zálohovacích kapacit

Diskové kapacity jsou poskytovány v rámci platformy x64 AzureStack prostřednictvím zdrojů StorageAccount a Managed disks v následujícím rozložení:

Storage (GB) pro ELK

Prostředí	Úložiště STOR1	Úložiště S3	Managed disks – x64 AzureStack
Produktivní prostředí	Celkový rozsah pro všechna prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Diskový prostor, resp. jeho změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy).		
Testovací prostředí/Vývojové prostředí*)			
Celkový rezervovaný objem	**31 000**	**26 000**	**61 120**
Poznámka *)	V rámci testovacího prostředí je provozováno i prostředí vývojové.		

Způsob realizace zálohování respektuje požadavky na dostupnost, výkonnost a umožňuje využít možnosti HW a technologií x64 AzureStack prostředí datových center SPCSS, zejména diskových polí a páskových knihoven. Zálohovací systém v rámci datových center SPCSS realizuje zálohování stanoveným způsobem a režimem nutným k zajištění SLA. Standardem je zálohování operačních systémů, vybraných souborových systémů, Name Space Kubernetes clusterů a databází.

Zálohování pro všechny moduly AISG – standard SPCSS (Mimo produkčních prostředí AISG AM a DaS, které jsou popsané níže):

Všechny systémy se pravidelně denně zálohují.

V rámci poskytování služby zálohování poskytuje Poskytovatel služby s následujícími parametry:

RTO 24 hodin

se týká obnovy do velikosti 1 TB. Nad 1 TB je obnova v závislosti na velikosti obnovovaných dat adekvátně prodloužena, pokud se Smluvní strany nedohodnou jinak.

RPO 24 h

maximální přípustná ztráta dat je 24 hodin, pokud se Smluvní strany nedohodnou jinak. Zálohy jsou spouštěny pravidelně denně, pokud se se Smluvní strany nedohodnou jinak. Standardní retence dat je 30 dní, resp. 28 dní pro databázové zálohy.

Definice:

RPO (Recovery Point Objective) - definuje, ke kterému bodu z minulosti lze obnovit data, respektive udává maximální dobu výpadku, a tedy i ztráty dat. RPO je tak klíčovým ukazatelem dostupnosti dat.

RTO (Recovery Time Objective) - vyjadřuje maximální dobu, za kterou by mělo dojít k zotavení po výpadku. Jedná se tak o důležitý ukazatel určující úroveň služby.

Specifické parametry RPO a RTO pro modul AISG DaS produkční prostředí:

Typ zálohy	Objem zdrojových serverů/db	RPO	Předpokládaný maximální RTO
Souborová na úrovni VMW	<1500 GB	24 hod	5 hod
Souborová na úrovni VMW	<100 GB	24 hod	2 hod
DB postgres	<400 GB	<30 min	5 hod

DB postgres	<100 GB	<30 min	2 hod

Dobu RTO není možné měřit jenom jako prostou dobu obnovy dat, je třeba započíst i dobu případného vytváření nové infrastruktury, instalace OS, aplikace, vytvoření uživatelů, koordinace prací s dodavatelem aplikace atp. Za předpokladu že se bude jednat o prostou obnovu dat bez nutnosti dalších součinností pak může být doba obnovy nižší než garantovaná.

Specifické parametry RPO a RTO pro modul AISG AM produkční prostředí:

Typ zálohy	Objem zdrojových serverů/db	RPO	Předpokládaný maximální RTO
Offline (Souborová záloha DB Postgres) pro DWH AMP1, AMD2	50 000 - 70 000 GB	24 hod	72 hod

Oblast – Provozní služby

2.2 Poskytování správy, servisní podpory SW a údržby HW

2.2.1 Poskytování správy operačních systémů

Služba je poskytována na následujících operačních systémech:

- RedHat 7.0 a vyšší;
- MS Windows: MS Windows Server Datacenter 2016 a vyšší;
- Kubernetes cluster 1.23 a vyšší.

Předpokladem služby pro licencované operační systémy je zajištění licence a maintenance OS.

Součástí služby není implementace a správa aplikačních komponent operačních systémů, respektive aplikačního SW přibaleného k základnímu OS, jako jsou například web servery, aplikační servery, middleware, nebo adresářové služby pro účely správy aplikačních uživatelů.

Služba zahrnuje následující činnosti:

- administrace operačních systémů, tzn. incident management, problem management a change management (vyjma změn aplikačních komponent – viz výše);
- aktualizace operačních systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost aplikací;
- upgrade operačního systému bude vždy řešen změnovým řízením, vlastní upgrade je součástí ceny, v rámci servisního zásahu mohou vzniknout vícenáklady, které nejsou zahrnuty v ceně služby;
- kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;
- provádění restartů operačních systémů dle požadavků Objednatele;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- součinnosti s případnou instalací a konfigurací nového software;
- instalace a údržba certifikátů doporučených dodavatelem aplikace pro zabezpečení přístupů na servery;
- úpravy výkonnostních parametrů systému;
- správa souborového systému (filesystem, přístupová práva a zaplněnost);
- testování změn provedených v OS;
- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);

- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele probíhá formou nástrojů typu sudo nebo jsou řízeny pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;
- Poskytovatel instaluje vždy minimální výchozí instalaci operačního systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace (balíčky, filesystemy, úpravy v konfiguračních souborech).

2.2.2 Poskytování správy databází

Služba je poskytována na následujících verzích databázového systému:

- PostgreSQL 10.x a vyšší.

Předpokladem služby pro licencované databázové systémy je zajištění licence a její maintenance.

Služba zahrnuje následující činnosti:

- administrace databázových systémů, tzn. incident management, problem management a change management;
- aktualizace databázových systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost databází;
- upgrade databázového systému bude vždy řešen změnovým řízením, vlastní upgrade je součástí ceny, v rámci servisního zásahu mohou vzniknout vícenáklady, které nejsou zahrnuty v ceně služby;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- úpravy výkonnostních parametrů databáze;
- testování změn provedených v databázi;
- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);
- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele je řízeno pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;
- Poskytovatel instaluje vždy minimální výchozí instalaci databázového systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace.

2.3 Zajišťování provozu bezpečného komunikačního rozhraní

V rámci zajišťování provozu bezpečného komunikačního rozhraní jsou typicky čerpány následující aktivity:

- připojení řešení z datových center SPCSS do internetu. Internetová konektivita je primárně realizována připojením do dvou nezávislých uzlů NIX dvěma nezávislými

optickými trasami o kapacitě 10 Gbps a sekundárně připojením dvěma nezávislými linkami 100 Mbps přes ISP;

- připojení řešení z datových center SPCSS do GOVBONE a CMS2. Připojení je zajištěno redundantními propoji v rámci DC SPCSS;
- propojení datových center DC Vápenka a DC Zeleneč – DCI;
- firewall a IPS;
- aplikační firewall a loadbalancer F5;
- VPN – vzdálené připojení do sítě SPCSS pomocí VPN, a to buď jako site-to-site VPN nebo remote-access VPN. Určeno pro dodavatele pro účely vzdálené správy aplikace.

Součástí výše uvedených položek je následující podpůrná infrastruktura a související služby, které jsou nezbytné pro provoz bezpečného propojení:

- plně redundantní síťová infrastruktura Poskytovatele;
- ochrana proti DoS a DDoS útokům;
- přiřazení a aktualizace bezpečnostních oprávnění uživatelům a zařízením v síti;
- aktualizace a opravy prvků síťové infrastruktury;
- vyhodnocování a optimalizace výkonu sítě a síťových prvků;
- zajištění dokumentace poskytovaných služeb a jejich technického nastavení pro potřeby Objednatele v takovém rozsahu, aby Objednatel byl schopen dokumentovat správu a provoz aplikační vrstvy ve všech provozních stavech podporovaných aplikací;
- řízení provozu a dohled nad kvalitou poskytované služby;
- řízení provozu a dohledu nad kvalitou poskytované služby vychází z požadavků příslušných standardů ITIL a norem ČSN ISO/IEC 20000.

2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb

2.4.1 Řízení provozu Systému zahrnuje zejména:

- koordinaci provozu HW a SW;
- řízení v oblasti rizik a kvality;
- řízení komunikace mezi dodavatelem aplikace a poskytovatelem;
- koordinaci změnových řízení v rámci poskytování služby.

2.4.2 Podpora poskytování služby prostřednictvím SW nástrojů SPCSS zahrnuje zejména:

- poskytování informací pro posouzení postupu řešení nedostupnosti a závad služby;
- procesní řízení získaných informací;
- SW a personální zajištění.

2.4.3 Dohled nad kvalitou poskytované služby zahrnuje zejména:

- trvalý provozní a bezpečnostní dohled;
- vyhodnocování SLA specifikované v Katalogovém listu.

Infrastruktura SPCSS splňuje veškeré požadavky na provozování AISG který je klasifikovaný jako Významný informační systém dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), včetně dalších požadavků prováděcích předpisů a nařízení. SPCSS je ve vztahu k MF významným dodavatelem a provozovatelem AISG.

Bezpečnost a dohledy na úrovni infrastruktury obsahuje bezpečnostní a provozní dohled na úrovni odpovídající charakteru části služby:

- poskytování výpočetního výkonu;
- poskytování správy operačních systémů;
- poskytování správy databází
- zajišťování provozu bezpečného komunikačního rozhraní.

Pravidelným měsíčním výstupem bezpečnostního dohledu je zpracování Zprávy o stavu bezpečnosti infrastruktury, která je součástí Zprávy

Poskytovatel se zavazuje tímto plnit povinnosti, které vychází ze shora uvedené legislativy.

Poskytovatel je povinen při poskytování infrastrukturních služeb plně implementovat a provádět ustanovení ZoKB a VoKB, zejména:

- zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti Významného informačního systému a vést o nich bezpečnostní dokumentaci;
- provádět opatření dle § 11 ZoKB;
- vést veškeré provozní a bezpečnostní záznamy infrastruktury, realizovat organizační a technická opatření požadovaná MF ke sběru a vyhodnocování záznamů dle vyhlášky č. 82/2018 Sb. vlastními prostředky;
- informovat Manažera kybernetické bezpečnosti MF o zranitelnostech, hrozbách a rizicích a jejich zvládání a pravidelných revizí;
- hlásit Manažeru kybernetické bezpečnosti MF o bezpečnostních hlášeních, kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech bez zbytečného odkladu;
- hlásit kybernetické bezpečnostní incidenty na Národní úřad pro kybernetickou a informační bezpečnost formou požadovanou VoKB a Manažera kybernetické bezpečnosti MF informovat a hlášení KBI na NÚKIB bez zbytečného odkladu o bezpečnostních incidentech, a to bezodkladně po jejich detekci;
- realizovat bezpečnostní opatření ke zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů po konzultaci s Manažera kybernetické bezpečnosti MF;
- umožnit přístup pro určené osoby Objednatele k řešení tiketů do systému Service Desk Poskytovatele, Manažerovi kybernetické bezpečnosti MF nebo dalším určeným osobám vzdálený přístup k záznamům týkajícím se AISG ELK v nástroji SIEM;
- komunikovat s MF kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty v rozsahu poskytovaných služeb nebo rozsahu, který by ovlivňoval poskytované služby;
- řídit bezpečnostní rizika AISG ELK;
- řídit kontinuitu provozu AISG ELK;
- předávat předem dohodnutou formou data, provozní údaje a informace vyžádané Objednatelem.

3 KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

3.1 Požadovaná měsíční dostupnost oblastí služby

Prostředí	**Dostupnost oblastí služby**	
	Poskytování výpočetního výkonu a zálohovacích kapacit	**Zajišťování provozu bezpečného komunikačního rozhraní**
		DaS
Produktivní	99,5 %	99,5 %
Preprodukční/Playground	95,0 %	95,0 %
Testovací	95,0 %	95,0 %
		AM

Produktivní	99,5 %	99,5 %
Testovací	95,0 %	95,0 %
Playground	95,0 %	95,0 %
Vývojové	95,0 %	95,0 %
		ELK
Produktivní	99,5 %	99,5 %
Testovací/Vývojové	95,0 %	95,0 %

Nedostupnost služby způsobená hardwarovou nebo jinou technickou závadou infrastruktury některého z prostředí pro provoz AISG (DaS, AM, ELK) se počítá od okamžiku zahájení nedostupnosti prostředí pro koncové uživatele do okamžiku odstranění této závady. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti prostředí pro koncové uživatele, počítá se nedostupnost služby od doby jejího nahlášení do Service Desku SPCSS.

Nedostupnost služby způsobená softwarovou závadou infrastruktury (nastavení systému, pravidla a prostupy firewalu, apod.) se počítá od okamžiku nahlášení nedostupnosti pro koncové uživatele IS v aplikaci **Service Desk SPCSS** do okamžiku odstranění této závady.

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 \times \frac{T - N}{T}$$

kde

D je dostupnost [%] v daném období.

T vyjadřuje fond provozní doby služby v daném období.

N vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky schválené mimořádné odstávky.

Servisní okna poskytované služby jsou ve čtvrtek od 20:00 do pátku 6:00 a pokud budou mít činnosti v servisním okně dopad do dostupnosti, bude Poskytovatel žádat o jejich schválení formou mimořádné odstávky.

3.2 Požadované lhůty pro obnovení služby

Prostředí	**Lhůta pro obnovení služby provozní době (7x24 hod) v hodinách**		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
			DaS
Produktivní	4	6	24
			ELK
Produktivní	4	6	24

Prostředí	Lhůta pro obnovení služby v běžné provozní době v hodinách		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
			DaS
Preprodukční/Playground	8	24	168
Testovací	24	72	168
			AM
Produktivní	4	6	24
Testovací	24	72	168
Playground	8	24	168
Vývojové	24	72	168
			ELK
Testovací/Vývojové	24	72	168

Kategorizace incidentů:

Incident kategorie A	Služba není použitelná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje jeho užívání většině nebo všem jejím uživatelům. Tento stav kritickým způsobem ohrožuje běžný provoz Objednatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody, a při tom neexistuje náhradní způsob zajištění poskytování služeb tohoto systému.
Incident kategorie B	Služba, je ve svých funkcích degradován tak, že tento stav zásadně omezuje běžný provoz Objednatele.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

3.3 Požadované lhůty pro obnovení služby pro vybrané komponenty

Lhůty pro obnovení služby v produktivním prostředí provozovaném v době konání plánovaného a odsouhlaseného Disaster Recovery testu (komponenty služby 2.1 Poskytování výpočetního výkonu, 2.3 Poskytování diskových a zálohovacích kapacit a 2.5 Zajišťování provozu bezpečného komunikačního rozhraní) jsou stejné jako v testovacím prostředí, tedy:

Prostředí	Lhůta pro obnovení služby v běžné provozní době v době konání plánovaného a odsouhlaseného Disaster Recovery testu		
	Incident kategorie A	Incident kategorie B	Incident kategorie C
DaS			
Produktivní	24	72	168
AM			
Produktivní	24	72	168
ELK			
Produktivní	24	72	168

4 CENA SLUŽBY

Prostředí: AISG Dozorová a Správní (DaS)			
Rozdělení služby dle odst. 2 tohoto katalogového listu	**Měsíční cena v Kč (MF/06)**		
	bez DPH	**DPH**	**s DPH**
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	187 817,00	39 441,57	227 258,57
2.2 Poskytování správy, servisní podpory SW a údržby HW (Provozní služba)	397 460,00	83 466,60	480 926,60
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	297 658,00	62 508,18	360 166,18
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	363 294,00	76 291,74	439 585,74
Celková měsíční cena	**1 246 229,00**	**261 708,09**	**1 507 937,09**

Prostředí: AISG Analytický modul (AM)			
Rozdělení služby dle odst. 2 tohoto katalogového listu	**Měsíční cena v Kč (MF/06)**		
	bez DPH	**DPH**	**s DPH**
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	2 371 047,00	497 919,87	2 868 966,87
2.2 Poskytování správy, servisní podpory SW a údržby HW (Provozní služba)	265 790,00	55 815,90	321 605,90
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	351 432,00	73 800,72	425 232,72
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	354 963,00	74 542,23	429 505,23
Celková měsíční cena	**3 343 232,00**	**702 078,72**	**4 045 310,72**

Prostředí: AISG ELK (ELK)			
Rozdělení služby dle odst. 2 tohoto katalogového listu	**Měsíční cena v Kč (MF/06)**		
	bez DPH	**DPH**	**s DPH**
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	436 849,00	91 738,29	528 587,29
2.2 Poskytování správy, servisní podpory SW a údržby HW (Provozní služba)	19 660,00	4 128,60	23 788,60
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	5 632,00	1 182,72	6 814,72
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	234 327,00	49 208,67	283 535,67
Celková měsíční cena	**696 468,00**	**146 258,28**	**842 726,28**

5 SMLUVNÍ POKUTY ZA NESPLNĚNÍ KVALITATIVNÍCH PARAMETRŮ POSKYTOVÁNÍ SLUŽBY

Za porušení kvalitativních parametrů, nedodržení dostupnosti služby dle pododst. 3.1 a nedodržení požadované lhůty pro obnovení služby dle pododst. 3.2 a pododst. 3.3, je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu vypočítanou za jednotlivé oblasti služby dle odst. 2 tohoto katalogového listu.

Název parametru	**Smluvní pokuta za porušení parametru služby v % z měsíční ceny uvedené za příslušnou podslužbu včetně DPH dle pododst. 4.1 a až 4.4 tohoto KL**	**Max. výše smluvní pokuty v % z měsíční ceny uvedené za příslušnou podslužbu včetně DPH dle pododst. 4.1 až 4.4 tohoto KL**	**Způsob výpočtu**
Dostupnost oblasti Služby	1	40	za každých započatých 15 minut nad povolený limit nedostupnosti nebo doby vyřešení incidentu
Doba vyřešení incidentu kategorie A	1	40	
Doba vyřešení incidentu kategorie B	0,5	15	
Doba vyřešení incidentu kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období.

Výše smluvní pokuty se při nedodržení dostupnosti konkrétního prostředí nebo nedodržení doby vyřešení incidentu vypočítá jako procento z celkové měsíční ceny podslužby dle tabulky v odst.4.1 až 4.4. tohoto katalogového listu.

MF/07	Zajištění a provoz produkčního prostředí IS EESS

1 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba bude poskytována pro produktivní prostředí IS EESS v režimu 24x7 hodin.

Celková doba je rozdělena na dvě části, běžnou provozní dobu (v kalendářních dnech od 6:00 hod do 20:00 hod) a rozšířenou provozní dobu (v kalendářních dnech od 20:00 hod do 6:00 hod).

Testovací prostředí bude poskytováno v režimu 8x5 hodin ve zkrácené provozní době, tj. v pracovních dnech od 8:00 do 16:00 hod.

Služba bude poskytovaná v rámci On-premise datových center SPCSS.

2 POPIS ROZSAHU SLUŽBY

Obsahem služby zajištění a provoz produkčního prostředí pro IS EESS v režimu podle odst. 1 tohoto Katalogového listu je zajištění bezpečného a spolehlivého provozu tohoto prostředí. V termínu zahájení poskytování služby Zajištění a provoz prostředí pro IS EESS podle tohoto katalogového listu má MF k dispozici HW infrastrukturu uvedeného prostředí pro provoz IS EESS.

Oblast – INFRA služby

2.1 Poskytování výpočetního výkonu

Služba bude realizována prostřednictvím zdrojů výpočetního výkonu VMWare, které má dostatečný výpočetní výkon, pro provozování IS EESS a požadovanou dostupnost.

Architektura infrastruktury umožňuje pro všechny prvky (servery, storage i komunikace) standardní škálování vertikálně i horizontálně s minimálním dopadem na provoz.

2.1.1 Výpočetní výkon na platformě x64 VMWare

Výpočetní výkon na platformě x64 VMWare je poskytován na technologiích Intel Xeon E5-2630 v4 a vyšší skrze optimalizované virtuální servery s operačními systémy Windows nebo Linux.

V ceně služby je zahrnuto i umístění v datovém centru včetně racku a energie.

Alokace je realizována prostředky virtualizační platformy a je v odpovědnosti Poskytovatele infrastruktury.

Alokace výpočetního výkonu je realizována prostředky virtualizační platformy a je v odpovědnosti Poskytovatele infrastruktury.

2.1.2 Celkové výkonnostní parametry všech prostředí on-premise IS EESS jsou uvedeny v následující tabulce:

Prostředí pro provoz IS EESS – Platforma x64 VMWare			
Prostředí	**CPU**	**RAM (GB)**	**Diskový prostor (GB)**
Produktivní	Celkový poskytovaný výkon pro jednotlivá prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou řízení provozu (viz Příloha č. 4 Smlouvy). Výkaz alokace výpočetního výkonu bude Poskytovatel předkládat Objednateli na vyžádání.		
Testovací			
Celkový rezervovaný výkon	**40**	**88**	**5 120**

2.1.3 Poskytování zálohovacích kapacit

Způsob realizace zálohování respektuje požadavky na dostupnost, výkonnost a umožňuje využít možnosti HW a technologií produkčního prostředí EESS, zejména diskových polí a páskových knihoven. Zálohovací systém realizuje zálohování stanoveným způsobem a režimem nutným k zajištění SLA. Standardem je zálohování operačních systémů, vybraných souborových systémů a databází.

Oblast – Provozní služby

2.2 Poskytování správy, servisní podpory SW a údržby HW

2.2.1 Poskytování správy operačních systémů

Služba je poskytována na následujících operačních systémech:

- MS Windows: MS Windows Server Datacenter 2019 a vyšší;
- RedHat 8.1 a vyšší.

Předpokladem služby pro licencované operační systémy je zajištění licence a maintenance OS.

Součástí služby není implementace a správa aplikačních komponent operačních systémů, respektive aplikačního SW přibaleného k základnímu OS, jako jsou například web servery, aplikační servery, middleware, nebo adresářové služby pro účely správy aplikačních uživatelů.

Služba zahrnuje následující činnosti:

- administrace operačních systémů, tzn. incident management, problem management a change management (vyjma změn aplikačních komponent – viz výše);
- aktualizace operačních systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost aplikací;
- kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;
- provádění restartů operačních systémů dle požadavků Objednatele;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- součinnosti s případnou instalací a konfigurací nového software;
- instalace a údržba certifikátů doporučených dodavatelem aplikace pro zabezpečení přístupů na servery;
- úpravy výkonnostních parametrů systému;
- správa souborového systému (filesystem, přístupová práva a zaplněnost);
- testování změn provedených v OS;
- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);
- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele probíhá formou nástrojů typu sudo nebo jsou řízeny pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;
- Poskytovatel instaluje vždy minimální výchozí instalaci operačního systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace (balíčky, filesystemy, úpravy v konfiguračních souborech).

2.2.2 Poskytování správy databází

Služba je poskytována na následujících verzích databázového systému:

- PostgreSQL 13.x a vyšší.

Předpokladem služby pro licencované databázové systémy je zajištění licence a její maintenance.

Služba zahrnuje následující činnosti:

- administrace databázových systémů, tzn. incident management, problem management a change management;
- aktualizace databázových systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost databází;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- úpravy výkonnostních parametrů databáze;
- testování změn provedených v databázi;
- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);
- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele je řízeno pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;
- Poskytovatel instaluje vždy minimální výchozí instalaci databázového systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace.

2.3 Zajišťování provozu bezpečného komunikačního rozhraní

V rámci zajišťování provozu bezpečného komunikačního rozhraní jsou typicky čerpány následující aktivity:

- připojení řešení z datových center SPCSS do internetu. Internetová konektivita je primárně realizována připojením do dvou nezávislých uzlů NIX dvěma nezávislými optickými trasami o kapacitě 10 Gbps a sekundárně připojením dvěma nezávislými linkami 100 Mbps přes ISP;
- připojení řešení z datových center SPCSS do GOVBONE. Připojení je zajištěno redundantními propoji v rámci DC SPCSS;
- propojení datových center DC Vápenka a DC Zeleneč – DCI;
- firewall a IPS;
- aplikační firewall a loadbalancer F5;
- VPN – vzdálené připojení do sítě SPCSS pomocí VPN, a to buď jako site-to-site VPN nebo remote-access VPN. Určeno pro dodavatele pro účely vzdálené správy aplikace.

Součástí výše uvedených položek je následující podpůrná infrastruktura a související služby, které jsou nezbytné pro provoz bezpečného propojení:

- plně redundantní síťová infrastruktura Poskytovatele;
- ochrana proti DoS a DdoS útokům;
- přiřazení a aktualizace bezpečnostních oprávnění uživatelům a zařízením v síti;
- aktualizace a opravy prvků síťové infrastruktury;
- vyhodnocování a optimalizace výkonu sítě a síťových prvků;

- zajištění dokumentace poskytovaných služeb a jejich technického nastavení pro potřeby Objednatele v takovém rozsahu, aby Objednatel byl schopen dokumentovat správu a provoz aplikační vrstvy ve všech provozních stavech podporovaných aplikací;
- řízení provozu a dohled nad kvalitou poskytované služby;
- řízení provozu a dohledu nad kvalitou poskytované služby vychází z požadavků příslušných standardů ITIL a norem ČSN ISO/IEC 20000.

2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb

2.4.1 Řízení provozu Systému zahrnuje zejména:

- koordinaci provozu HW a SW;
- řízení v oblasti rizik a kvality;
- řízení komunikace mezi dodavatelem aplikace a poskytovatelem;
- koordinaci změnových řízení v rámci poskytování služby;

2.4.2 Podpora poskytování služby prostřednictvím SW nástrojů SPCSS zahrnuje zejména:

- poskytování informací pro posouzení postupu řešení nedostupnosti a závad služby;
- procesní řízení získaných informací;
- SW a personální zajištění.

2.4.3 Dohled nad kvalitou poskytované služby zahrnuje zejména:

- trvalý provozní a bezpečnostní dohled;
- vyhodnocování SLA specifikované v Katalogovém listu.

Infrastruktura SPCSS splňuje veškeré požadavky na provozování IS EESS který poskytuje podporu významným informačním systémům klasifikovaným dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), včetně dalších požadavků prováděcích předpisů a nařízení a SPCSS se zavazuje s EESS nakládat jako s významným informačním systémem. Z tohoto pohledu je pro MF významným dodavatelem ve vztahu k EESS.

Bezpečnost a dohledy na úrovni infrastruktury obsahuje bezpečnostní a provozní dohled na úrovni odpovídající charakteru části služby:

- poskytování výpočetního výkonu;
- poskytování správy operačních systémů;
- poskytování správy databází;
- zajišťování provozu bezpečného komunikačního rozhraní.

Pravidelným měsíčním výstupem bezpečnostního dohledu je zpracování Zprávy o stavu bezpečnosti infrastruktury, která je součástí Zprávy.

Poskytovatel se zavazuje tímto plnit povinnosti, které vychází ze shora uvedené legislativy.

Poskytovatel je povinen při poskytování infrastrukturních služeb plně implementovat a provádět ustanovení ZoKB a VoKB, zejména:

- zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti Významného informačního systému a vést o nich bezpečnostní dokumentaci;
- provádět opatření dle § 11 ZoKB;
- vést veškeré provozní a bezpečnostní záznamy infrastruktury, realizovat organizační a technická opatření požadovaná MF ke sběru a vyhodnocování záznamů dle vyhlášky č. 82/2018 Sb. Vlastními prostředky;
- informovat Manažera kybernetické bezpečnosti MF o zranitelnostech, hrozbách a rizicích a jejich zvládání a pravidelných revizí;

- hlásit Manažeru kybernetické bezpečnosti MF o bezpečnostních hlášeních, kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech bez zbytečného odkladu;
- realizovat bezpečnostní opatření ke zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů po konzultaci s Manažera kybernetické bezpečnosti MF;
- umožnit přístup pro určené osoby Objednatele k řešení tiketů do systému Service Desk Poskytovatele, Manažerovi kybernetické bezpečnosti MF nebo dalším určeným osobám vzdálený přístup k záznamům týkajícím se IS EESS v nástroji SIEM;
- komunikovat s MF kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty v rozsahu poskytovaných služeb nebo rozsahu, který by ovlivňoval poskytované služby;
- řídit bezpečnostní rizika IS EESS;
- řídit kontinuitu provozu IS EESS;
- předávat předem dohodnutou formou data, provozní údaje a informace vyžádané Objednatelem.

3 KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

3.1 Požadovaná měsíční dostupnost oblastí služby

Prostředí	Dostupnost oblastí služby	
	Poskytování výpočetního výkonu a zálohovacích kapacit	**Zajišťování provozu bezpečného komunikačního rozhraní**
Produktivní	99,5 %	99,5 %
Testovací	95,0 %	95,0 %
Vývojové	95,0 %	95,0 %

Nedostupnost služby způsobená hardwarovou nebo jinou technickou závadou infrastruktury některého z prostředí pro provoz IS EESS se počítá od okamžiku zahájení nedostupnosti IS EESS pro koncové uživatele do okamžiku odstranění této závady. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti IS EESS pro koncové uživatele, počítá se nedostupnost služby od doby jejího nahlášení do Service Desku SPCSS.

Nedostupnost služby způsobená softwarovou závadou infrastruktury IS EESS (nastavení systému, pravidla a prostupy firewalu, apod.) se počítá od okamžiku nahlášení nedostupnosti IS EESS pro koncové uživatele do okamžiku odstranění této závady.

Za **nahlášení nedostupnosti služby** se považuje založení odpovídajícího servisního hlášení v aplikaci **Service Desk SPCSS** (servicedesk.spcss.cz).

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 \times \frac{T - N}{T}$$

kde

D je dostupnost [%] v daném období.

T vyjadřuje fond provozní doby služby v daném období.

N vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky schválené mimořádné odstávky.

Servisní okna poskytované služby jsou ve čtvrtek od 20:00 do 6:00 a pokud budou mít činnosti v servisním okně dopad do dostupnosti, bude Poskytovatel žádat o jejich schválení formou mimořádné odstávky.

3.2 Požadované lhůty pro obnovení služby

Prostředí	Lhůta pro obnovení služby v běžné provozní době v hodinách		
	Incident kategorie A	Incident kategorie B	Incident kategorie C
Produktivní	4	6	24
Vývojové	24	72	168
Testovací	24	72	168

Kategorizace incidentů:

Incident kategorie A	Služba není použitelná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje jeho užívání většině nebo všem jejím uživatelům. Tento stav kritickým způsobem ohrožuje běžný provoz Objednatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody, a při tom neexistuje náhradní způsob zajištění poskytování služeb tohoto systému.
Incident kategorie B	Služba, je ve svých funkcích degradován tak, že tento stav zásadně omezuje běžný provoz Objednatele.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

3.3 Požadované lhůty pro obnovení služby pro vybrané komponenty

Lhůty pro obnovení služby v produktivním prostředí provozovaném v době konání plánovaného a odsouhlaseného Disaster Recovery testu (komponenty služby 2.1 Poskytování výpočetního výkonu a zálohování a 2.3 zajišťování provozu bezpečného komunikačního rozhraní) jsou stejné jako v testovacím prostředí, tedy:

Prostředí	Lhůta pro obnovení služby v běžné provozní době v době konání plánovaného a odsouhlaseného Disaster Recovery testu		
	Incident kategorie A	Incident kategorie B	Incident kategorie C
Produktivní	24	72	168

4 CENA SLUŽBY

Rozdělení služby dle odst. 2 tohoto katalogového listu	Měsíční cena v Kč (MF/07)		
	bez DPH	DPH	s DPH
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	23 878,00	5 014,38	28 892,38
2.2 Poskytování správy, servisní podpory SW a údržby HW (Provozní služba)	81 242,00	17 060,82	98 302,82

Rozdělení služby dle odst. 2 tohoto katalogového listu	Měsíční cena v Kč (MF/07)		
	bez DPH	DPH	s DPH
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	112 191,00	23 560,11	135 751,11
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	132 134,00	27 748,14	159 882,14
Celková měsíční cena	**349 445,00**	**73 383,45**	**422 828,45**

4.1 Smluvní pokuty za nesplnění kvalitativních parametrů poskytování služby

Za porušení kvalitativních parametrů, nedodržení dostupnosti služby dle pododst. 3.1 a nedodržení požadované lhůty pro obnovení služby dle pododst. 3.2 a pododst. 3.3, je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu vypočítanou za jednotlivé oblasti služby dle odst. 2 tohoto katalogového listu.

Název parametru	Smluvní pokuta za porušení parametru služby v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Max. výše smluvní pokuty v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Způsob výpočtu
Dostupnost oblasti Služby	1	40	za každých započatých 15 minut nad povolený limit nedostupnosti nebo doby vyřešení incidentu
Doba vyřešení incidentu kategorie A	1	40	
Doba vyřešení incidentu kategorie B	0,5	15	
Doba vyřešení incidentu kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období.

Výše smluvní pokuty se při nedodržení dostupnosti konkrétního prostředí nebo nedodržení doby vyřešení incidentu vypočítá jako procento z celkové měsíční ceny služby dle tabulky v odst. 4 tohoto katalogového listu.

MF/08	Zajištění a provoz produkčního prostředí ARES

1 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba bude poskytována pro všechna 3 prostředí v režimu 24x7 hodin.

Celková doba je rozdělena na dvě části, běžnou provozní dobu (v kalendářních dnech od 6:00 hod do 20:00 hod) a rozšířenou provozní dobu (v kalendářních dnech od 20:00 hod do 6:00 hod).

Služba bude poskytovaná hybridně – rozdělena mezi privátní cloud MS AzureStack HUB provozovaný v rámci On-premise datových center SPCSS a poskytovatele cloudových služeb MS Azure. Jednotlivá prostředí budou poskytována v následujícím rozsahu:

Prostředí	Období poskytování
Produkční	Po celou dobu poskytování služby.
Vývojové	Prvních 12 měsíců poskytování služby, v následujícím období dle požadavku Objednatele.
Testovací	Prvních 12 měsíců poskytování služby, v následujícím období dle požadavku Objednatele.

2 POPIS ROZSAHU SLUŽBY

Obsahem služby je zajištění bezpečného a spolehlivého provozu produkčního, testovacího a vývojového prostředí pro IS ARES v režimu podle odst. 1 tohoto Katalogového listu. V termínu zahájení poskytování služby podle tohoto katalogového listu má MF k dispozici HW infrastrukturu všech výše uvedených prostředí.

2.1 Poskytování výpočetního výkonu

Služba bude realizována prostřednictvím zdrojů výpočetního výkonu a služeb x64 AzureStack a public cloudu MS AZURE, které mají dostatečný výpočetní výkon, pro provozování IS ARES s požadovanou dostupností.

Architektura infrastruktury umožňuje pro všechny prvky (servery, storage i komunikace) standardní škálování vertikálně i horizontálně s minimálním dopadem na provoz.

Oblast – Infra služby

2.1.1 Výpočetní výkon na platformě x64 AzureStack

Výpočetní výkon na platformě x64 AzureStack je poskytován v rámci obou datových center SPCSS, na technologiích Intel® Xeon® Gold 6248 a vyšší prostřednictvím optimalizovaných virtuálních serverů Cisco UCS C2420 M5. V ceně služby je zahrnuto i umístění v datovém centru včetně racku a zálohovaného napájení a chlazení.

Alokace výpočetního výkonu je realizována prostředky virtualizační platformy a je v odpovědnosti Poskytovatele infrastruktury.

2.1.2 Celkové výkonnostní parametry všech prostředí on-premise IS ARES jsou uvedeny v následující tabulce:

Prostředí pro provoz IS ARES – Platforma x64 AzureStack			
Prostředí	**vCPU LIN**	**vCPU WIN**	**RAM (GB)**
Produktivní	752	32	1 736
Testovací	232	8	600
Vývojové	44	2	161
Celkový rezervovaný výkon	**1 028**	**42**	**2 497**
Poznámka	Celkový rozsah pro všechna tři prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy). Výkaz alokace výpočetního výkonu bude Poskytovatel předkládat Objednateli na vyžádání.		

Oblast – Cloudové služby

2.1.3 Výpočetní výkon na platformě public cloud MS Azure

Výpočetní výkon na platformě public cloud MS Azure je poskytován v rámci regionu West Europe a na základě zvoleného příslušného plánu výpočetního výkonu. Detailní HW specifikace je popsána v jednotlivých oblastech služby.

Prostředí pro provoz IS ARES – Platforma MS AZURE		
Prostředí	**vCPU LIN**	**RAM (GB)**
Produktivní	120	416
Testovací	36	144
Vývojové	24	96
Celkový rezervovaný výkon	**180**	**656**
Poznámka	Celkový rozsah pro všechna tři prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy). Výkaz alokace výpočetního výkonu bude Poskytovatel předkládat Objednateli na vyžádání.	

2.1.4 Poskytování diskových a zálohovacích kapacit

Diskové kapacity jsou poskytovány v rámci jednotlivých cloud platforem prostřednictvím zdrojů Storage Account v následujícím rozložení:

Diskové kapacity pro IS ARES – Platforma MS AZURE region West Europe		
Prostředí	**Blob Storage**	**Managed disks**
Produktivní	6 500	-
Testovací	3 100	-
Vývojové	700	384
Celkový rezervovaný objem	**10 300**	**384**
Poznámka	Celkový rozsah pro všechna tři prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy). Výkaz alokace výpočetního výkonu bude Poskytovatel předkládat Objednateli na vyžádání.	

Diskové kapacity pro IS ARES – Platforma x64 AzureStack		
Prostředí	**Blob Storage**	**Managed disks**
Produktivní	14 096	-
Testovací	7 992	-
Vývojové	1 006	1 408
Celkový rezervovaný objem	**23 094**	**1 408**

Poznámka	Celkový rozsah pro všechna tři prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy). Výkaz alokace výpočetního výkonu bude Poskytovatel předkládat Objednateli na vyžádání.

Způsob realizace zálohování respektuje požadavky na dostupnost, výkonnost a umožňuje využít možnosti HW a technologií x64 AzureStack prostředí datových center SPCSS, zejména diskových polí a páskových knihoven. Zálohovací systém v rámci datových center SPCSS realizuje zálohování stanoveným způsobem a režimem nutným k zajištění SLA. Standardem je zálohování operačních systémů, vybraných souborových systémů, Name Space Kubernetes clusterů a databází.

Oblast – Provozní služby

2.2 Poskytování správy, servisní podpory SW a údržby HW

2.2.1 Poskytování správy operačních systémů

Služba je poskytována na následujících operačních systémech:

- MS Windows: MS Windows Server Datacenter 2019 a vyšší;
- Kubernetes cluster 1.23 a vyšší.

Předpokladem služby pro licencované operační systémy je zajištění licence a maintenance OS.

Součástí služby není implementace a správa aplikačních komponent operačních systémů, respektive aplikačního SW přibaleného k základnímu OS, jako jsou například web servery, aplikační servery, middleware, nebo adresářové služby pro účely správy aplikačních uživatelů.

Služba zahrnuje následující činnosti:

- administrace operačních systémů, tzn. incident management, problem management a change management (vyjma změn aplikačních komponent – viz výše);
- aktualizace operačních systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost aplikací;
- kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;
- provádění restartů operačních systémů dle požadavků Objednatele;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- součinnosti s případnou instalací a konfigurací nového software;
- instalace a údržba certifikátů doporučených dodavatelem aplikace pro zabezpečení přístupů na servery;
- úpravy výkonnostních parametrů systému;
- správa souborového systému (filesystem, přístupová práva a zaplněnost);
- testování změn provedených v OS;

- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);
- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele probíhá formou nástrojů typu sudo nebo jsou řízeny pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;
- Poskytovatel instaluje vždy minimální výchozí instalaci operačního systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace (balíčky, filesystemy, úpravy v konfiguračních souborech).

2.2.2 Poskytování správy databází

Služba je poskytována na následujících verzích databázového systému:

- MS SQL server 2019 Enterprise;
- MS SQL server 2019 Developer.

Předpokladem služby pro licencované databázové systémy je zajištění licence a její maintenance.

Služba zahrnuje následující činnosti:

- administrace databázových systémů, tzn. incident management, problem management a change management;
- aktualizace databázových systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost databází;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- úpravy výkonnostních parametrů databáze;
- testování změn provedených v databázi;
- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);
- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele je řízeno pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;
- Poskytovatel instaluje vždy minimální výchozí instalaci databázového systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace.

2.3 Zajišťování provozu bezpečného komunikačního rozhraní

V rámci zajišťování provozu bezpečného komunikačního rozhraní jsou typicky čerpány následující aktivity:

- připojení řešení z datových center SPCSS do internetu. Internetová konektivita je primárně realizována připojením do dvou nezávislých uzlů NIX dvěma nezávislými

optickými trasami o kapacitě 10 Gbps a sekundárně připojením dvěma nezávislými linkami 100 Mbps přes ISP;

- připojení řešení z datových center SPCSS do GOVBONE a CMS2. Připojení je zajištěno redundantními propoji v rámci DC SPCSS;
- propojení datových center DC Vápenka a DC Zeleneč – DCI;
- firewall a IPS;
- aplikační firewall a loadbalancer F5;
- VPN – vzdálené připojení do sítě SPCSS pomocí VPN, a to buď jako site-to-site VPN nebo remote-access VPN. Určeno pro dodavatele pro účely vzdálené správy aplikace.

Součástí výše uvedených položek je následující podpůrná infrastruktura a související služby, které jsou nezbytné pro provoz bezpečného propojení:

- plně redundantní síťová infrastruktura Poskytovatele;
- ochrana proti DoS a DdoS útokům;
- přiřazení a aktualizace bezpečnostních oprávnění uživatelům a zařízením v síti;
- aktualizace a opravy prvků síťové infrastruktury;
- vyhodnocování a optimalizace výkonu sítě a síťových prvků;
- zajištění dokumentace poskytovaných služeb a jejich technického nastavení pro potřeby Objednatele v takovém rozsahu, aby Objednatel byl schopen dokumentovat správu a provoz aplikační vrstvy ve všech provozních stavech podporovaných aplikací;
- řízení provozu a dohled nad kvalitou poskytované služby;
- řízení provozu a dohledu nad kvalitou poskytované služby vychází z požadavků příslušných standardů ITIL a norem ČSN ISO/IEC 20000.

2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb

2.4.1 Řízení provozu Systému zahrnuje zejména:

- koordinaci provozu HW a SW;
- řízení v oblasti rizik a kvality;
- řízení komunikace mezi dodavatelem aplikace a poskytovatelem;
- koordinaci změnových řízení v rámci poskytování služby.

2.4.2 Podpora poskytování služby prostřednictvím SW nástrojů SPCSS zahrnuje zejména:

- poskytování informací pro posouzení postupu řešení nedostupnosti a závad služby;
- procesní řízení získaných informací;
- SW a personální zajištění.

2.5 Dohled nad kvalitou poskytované služby zahrnuje zejména:

- trvalý provozní a bezpečnostní dohled;
- vyhodnocování SLA specifikované v Katalogovém listu.

Infrastruktura SPCSS splňuje veškeré požadavky na provozování IS ARES který je klasifikovaný jako Významný informační systém dle zákona č. 181/2014 Sb. O kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), včetně dalších požadavků prováděcích předpisů a nařízení. SPCSS je ve vztahu k MF významným dodavatelem a provozovatelem IS ARES.

Bezpečnost a dohledy na úrovni infrastruktury obsahuje bezpečnostní a provozní dohled na úrovni odpovídající charakteru části služby:

- poskytování výpočetního výkonu;

- poskytování správy operačních systémů;
- poskytování správy databází;
- zajišťování provozu bezpečného komunikačního rozhraní.

Pravidelným měsíčním výstupem bezpečnostního dohledu je zpracování Zprávy o stavu bezpečnosti infrastruktury, která je součástí Zprávy.

Poskytovatel se zavazuje tímto plnit povinnosti, které vychází ze shora uvedené legislativy.

Poskytovatel je povinen při poskytování infrastrukturních služeb plně implementovat a provádět ustanovení ZoKB a VoKB, zejména:

- zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti Významného informačního systému a vést o nich bezpečnostní dokumentaci;
- provádět opatření dle § 11 ZoKB;
- vést veškeré provozní a bezpečnostní záznamy infrastruktury, realizovat organizační a technická opatření požadovaná MF ke sběru a vyhodnocování záznamů dle vyhlášky č. 82/2018 Sb. Vlastními prostředky;
- informovat Manažera kybernetické bezpečnosti MF o zranitelnostech, hrozbách a rizicích a jejich zvládání a pravidelných revizí;
- hlásit Manažeru kybernetické bezpečnosti MF o bezpečnostních hlášeních, kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech bez zbytečného odkladu;
- hlásit kybernetické bezpečnostní incidenty na Národní úřad pro kybernetickou a informační bezpečnost formou požadovanou VoKB a Manažera kybernetické bezpečnosti MF informovat a hlášení KBI na NÚKIB bez zbytečného odkladu o bezpečnostních incidentech, a to bezodkladně po jejich detekci;
- realizovat bezpečnostní opatření ke zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů po konzultaci s Manažera kybernetické bezpečnosti MF;
- umožnit přístup pro určené osoby Objednatele k řešení tiketů do systému Service Desk Poskytovatele, Manažerovi kybernetické bezpečnosti MF nebo dalším určeným osobám vzdálený přístup k záznamům týkajícím se IS ARES v nástroji SIEM;
- komunikovat s MF kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty v rozsahu poskytovaných služeb nebo rozsahu, který by ovlivňoval poskytované služby;
- řídit bezpečnostní rizika IS ARES;
- řídit kontinuitu provozu IS ARES;
- předávat předem dohodnutou formou data, provozní údaje a informace vyžádané Objednatelem.

3 KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

3.1 Požadovaná měsíční dostupnost oblastí služby

Prostředí	Dostupnost oblastí služby	
	Poskytování výpočetního výkonu a zálohovacích kapacit	Zajišťování provozu bezpečného komunikačního rozhraní
Produktivní	99,5 %	99,5 %
Testovací	95,0 %	95,0 %
Vývojové	95,0 %	95,0 %

Nedostupnost služby způsobená hardwarovou nebo jinou technickou závadou infrastruktury některého z prostředí pro provoz IS ARES se počítá od okamžiku zahájení

nedostupnosti IS ARES pro koncové uživatele do okamžiku odstranění této závady. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti IS ARES pro koncové uživatele, počítá se nedostupnost služby od doby jejího nahlášení do Service Desku SPCSS.

Za **nahlášení nedostupnosti služby** se považuje založení odpovídajícího servisního hlášení v aplikaci **Service Desk SPCSS** (servicedesk.spcss.cz).

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 \times \frac{T - N}{T}$$

kde

D je dostupnost [%] v daném období.

T vyjadřuje fond provozní doby služby v daném období.

N vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky schválené mimořádné odstávky.

Servisní okna poskytované služby jsou ve čtvrtek od 20:00 do 6:00 a pokud budou mít činnosti v servisním okně dopad do dostupnosti, bude Poskytovatel žádat o jejich schválení formou mimořádné odstávky.

3.2 Požadované lhůty pro obnovení služby

Prostředí	Lhůta pro obnovení služby v běžné provozní době v hodinách		
	Incident kategorie A	Incident kategorie B	Incident kategorie C
Produktivní	4	6	24
Vývojové	24	72	168
Testovací	24	72	168

Kategorizace incidentů:

Incident kategorie A	Služba není použitelná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje jeho užívání většině nebo všem jejím uživatelům. Tento stav kritickým způsobem ohrožuje běžný provoz Objednatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody, a při tom neexistuje náhradní způsob zajištění poskytování služeb tohoto systému.
Incident kategorie B	Služba, je ve svých funkcích degradován tak, že tento stav zásadně omezuje běžný provoz Objednatele.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

3.3 Požadované lhůty pro obnovení služby pro vybrané komponenty

Lhůty pro obnovení služby v produktivním prostředí provozovaném v době konání plánovaného a odsouhlaseného Disaster Recovery testu (komponenty služby 2.1 Poskytování výpočetního výkonu a zálohování a 2.3 zajišťování provozu bezpečného komunikačního rozhraní) jsou stejné jako v testovacím prostředí, tedy:

Prostředí	Lhůta pro obnovení služby v běžné provozní době v době konání plánovaného a odsouhlaseného Disaster Recovery testu		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Produktivní	24	72	168

4 CENA SLUŽBY

ARES produkční prostředí			
Rozdělení služby dle odst. 2 tohoto katalogového listu	**Měsíční cena v Kč (MF/08)**		
	bez DPH	**DPH**	**s DPH**
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu (Cloudová služba)	Cena za Cloudové služby je stanovena dle skutečně čerpaného plnění za jeden kalendářní měsíc poskytování Cloudových služeb. Vyúčtování Cloudové služby bude provedeno dle mechanismu, který je stanoven v tomto katalogovém listu.		
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	397 489,00	83 472,69	480 961,69
2.2 Poskytování správy, servisní podpory SW a údržby HW (Provozní služba)	278 978,00	58 585,38	337 563,38
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	34 455,00	7 235,55	41 690,55
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	386 505,00	81 166,05	467 671,05
Celková měsíční cena	**1 097 427,00**	**230 459,67**	**1 327 886,67**

ARES vývojové prostředí (vyúčtování proběhne v souladu s čl. VI. Odst. 6.9 Smlouvy)			
Rozdělení služby dle odst. 2 tohoto katalogového listu	**Měsíční cena v Kč (MF/08)**		
	bez DPH	**DPH**	**s DPH**
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu (Cloudová služba)	Cena za Cloudové služby je stanovena dle skutečně čerpaného plnění za jeden kalendářní měsíc poskytování Cloudových služeb. Vyúčtování Cloudové služby bude provedeno dle mechanismu, který je stanoven v tomto katalogovém listu.		
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	31 494,00	6 613,74	38 107,74
2.2 Poskytování správy, servisní podpory SW a údržby HW (Provozní služba)	13 915,00	2 922,15	16 837,15
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	1 914,00	401,94	2 315,94

ARES vývojové prostředí (vyúčtování proběhne v souladu s čl. VI. Odst. 6.9 Smlouvy)			
Rozdělení služby dle odst. 2 tohoto katalogového listu	**Měsíční cena v Kč (MF/08)**		
	bez DPH	**DPH**	**s DPH**
Měsíční cena v období od 01.04.2025 do 31.03.2028			
Celková měsíční cena	**47 323,00**	**9 937,83**	**57 260,83**

ARES testovací prostředí (vyúčtování proběhne v souladu s čl. VI. Odst. 6.9 Smlouvy)			
Rozdělení služby dle odst. 2 tohoto katalogového listu	**Měsíční cena v Kč (MF/08)**		
	bez DPH	**DPH**	**s DPH**
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu (Cloudová služba)	Cena za Cloudové služby je stanovena dle skutečně čerpaného plnění za jeden kalendářní měsíc poskytování Cloudových služeb. Vyúčtování Cloudové služby bude provedeno dle mechanismu, který je stanoven v tomto katalogovém listu.		
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	138 811,00	29 150,31	167 961,31
2.2 Poskytování správy, servisní podpory SW a údržby HW (Provozní služba)	24 110,00	5 063,10	29 173,10
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	4 905,00	1 030,05	5 935,05
Celková měsíční cena	**167 826,00**	**35 243,46**	**203 069,46**

Cena je stanovena dle skutečného čerpání Cloudových služeb, tj. Azure jednotek pro jednotlivé Informační Systémy, resp. jejich jednotlivá prostředí.

Pro účely fakturace Cloudových služeb je stanoveno, že 1 Azure Jednotka = 1 Euro. Kurz Euro dle nákupu Azure Jednotek Poskytovatelem je stanoven na 25,155 Kč/Euro a je pro Objednatele závazný, pokud nebude ze strany Poskytovatele oznámen Objednateli nový kurz Euro za nákup Azure jednotek, a to prostřednictvím příslušného Záznamu. V každém měsíčním Záznamu bude Poskytovatelem uveden kurz Euro, za který byly nakoupeny předmětné Azure jednotky a tento kurz je pro Smluvní strany závazný. Poskytovatel se zavazuje v Záznamu vždy uvést konkrétní den, ke kterému došlo ke změně kurzu Euro. Pro vyloučení pochybností Smluvní strany výslovně uvádějí, že tato změna kurzu není důvodem k uzavření dodatku ke Smlouvě a bude provedena jednostranně ze strany Poskytovatele.

5 SMLUVNÍ POKUTY ZA NESPLNĚNÍ KVALITATIVNÍCH PARAMETRŮ POSKYTOVÁNÍ SLUŽBY

Za porušení kvalitativních parametrů, nedodržení dostupnosti služby dle pododst. 3.1 a nedodržení požadované lhůty pro obnovení služby dle pododst. 3.2 a pododst. 3.3, je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu vypočítanou za jednotlivé oblasti služby dle odst. 2 tohoto katalogového listu.

Název parametru	Smluvní pokuta za porušení parametru služby v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Max. výše smluvní pokuty v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Způsob výpočtu
Dostupnost oblasti Služby	1	40	za každých započatých 15 minut nad povolený limit nedostupnosti nebo doby vyřešení incidentu
Doba vyřešení incidentu kategorie A	1	40	
Doba vyřešení incidentu kategorie B	0,5	15	
Doba vyřešení incidentu kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období.

Výše smluvní pokuty se při nedodržení dostupnosti konkrétního prostředí nebo nedodržení doby vyřešení incidentu vypočítá jako procento z celkové měsíční ceny služby dle tabulky v odst. 4 tohoto katalogového listu.

MF/09	Zajištění a provoz prostředí pro OpenData

1 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba bude poskytována pro prostředí OpenData v režimu 24x7 hodin s dobou podpory v pracovní dny 8:00 – 17:00. Služba je poskytovaná v rámci On-premise datových center SPCSS.

Celková doba je rozdělena na dvě části, běžnou provozní dobu (v kalendářních dnech od 6:00 hod do 20:00 hod) a rozšířenou provozní dobu (v kalendářních dnech od 20:00 hod do 6:00 hod).

2 POPIS ROZSAHU SLUŽBY

Obsahem služby zajištění a provoz produkčního prostředí pro OpenData v režimu podle odst. 1 tohoto Katalogového listu je zajištění bezpečného a spolehlivého provozu tohoto prostředí. V termínu zahájení poskytování služby Zajištění a provoz prostředí pro OpenData podle tohoto katalogového listu má MF k dispozici HW infrastrukturu uvedeného prostředí pro provoz OpenData.

Oblast – Infra služby

2.1 Poskytování výpočetního výkonu

Služba bude realizována prostřednictvím zdrojů výpočetního výkonu VMWare, které má dostatečný výpočetní výkon, pro provozování OpenData a požadovanou dostupnost.

Architektura infrastruktury umožňuje pro všechny prvky (servery, storage i komunikace) standardní škálování vertikálně i horizontálně s minimálním dopadem na provoz.

2.1.1 Výpočetní výkon na platformě x64

Výpočetní výkon na platformě x64 je poskytován na technologiích Intel Xeon E5-2630 v4 a vyšší skrze optimalizované virtuální servery s operačními systémy Windows nebo Linux.

V ceně služby je zahrnuto i umístění v datovém centru včetně racku a energie.

Alokace je realizována prostředky virtualizační platformy a je v odpovědnosti Poskytovatele infrastruktury.

Alokace výpočetního výkonu je realizována prostředky virtualizační platformy a je v odpovědnosti Poskytovatele infrastruktury.

Celkové výkonnostní parametry všech prostředí on-premise OpenData jsou uvedeny v následující tabulce:

Prostředí pro provoz OpenData – Platforma x64			
Prostředí	**CPU**	**RAM (GB)**	**Diskový prostor (GB)**
Produktivní	Celkový poskytovaný výkon pro jednotlivá prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz Příloha č. 4 Smlouvy). Výkaz alokace výpočetního výkonu bude Poskytovatel předkládat Objednateli na vyžádání.		
Celkový rezervovaný výkon	**8**	**16**	**537**

2.1.2 Poskytování zálohovacích kapacit

Způsob realizace zálohování respektuje požadavky na dostupnost, výkonnost a umožňuje využít možnosti HW a technologií produkčního prostředí OpenData, zejména diskových polí a páskových knihoven. Zálohovací systém realizuje zálohování stanoveným způsobem a režimem nutným k zajištění SLA. Standardem je zálohování operačních systémů, vybraných souborových systémů a databází.

Požadavky na RPO, RTO a zálohovací plány jsou uvedeny v provozní dokumentaci a jsou schvalovány řídícími orgány provozu.

Oblast – Provozní služby

2.2 Poskytování správy, servisní podpory SW a údržby HW

2.2.1 Poskytování správy operačních systémů

Služba je poskytována na následujících operačních systémech:

- Centos 7.0 a vyšší.

Předpokladem služby pro licencované operační systémy je zajištění licence a maintenance OS.

Součástí služby není implementace a správa aplikačních komponent operačních systémů, respektive aplikačního SW přibaleného k základnímu OS, jako jsou například web servery, aplikační servery, middleware, nebo adresářové služby pro účely správy aplikačních uživatelů.

Služba zahrnuje následující činnosti:

- administrace operačních systémů, tzn. incident management, problem management a change management (vyjma změn aplikačních komponent – viz výše);
- aktualizace operačních systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost aplikací;
- kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;
- provádění restartů operačních systémů dle požadavků Objednatele;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- součinnosti s případnou instalací a konfigurací nového software;
- instalace a údržba certifikátů doporučených dodavatelem aplikace pro zabezpečení přístupů na servery;
- úpravy výkonnostních parametrů systému;

- správa souborového systému (filesystem, přístupová práva a zaplněnost);
- testování změn provedených v OS;
- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);
- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele probíhá formou nástrojů typu sudo nebo jsou řízeny pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;
- Poskytovatel instaluje vždy minimální výchozí instalaci operačního systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace (balíčky, filesystémy, úpravy v konfiguračních souborech).

2.2.2 Poskytování správy databází

Služba je poskytována na následujících verzích databázového systému:

- PostgreSQL 11.x a vyšší.

Předpokladem služby pro licencované databázové systémy je zajištění licence a její maintenance.

Služba zahrnuje následující činnosti:

- administrace databázových systémů, tzn. incident management, 70roblém management a change management;
- aktualizace databázových systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost databází;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- úpravy výkonnostních parametrů databáze;
- testování změn provedených v databázi;
- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);
- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele je řízeno pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;
- Poskytovatel instaluje vždy minimální výchozí instalaci databázového systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace.

2.3 Zajišťování provozu bezpečného komunikačního rozhraní

V rámci zajišťování provozu bezpečného komunikačního rozhraní jsou typicky čerpány následující aktivity:

- připojení řešení z datových center SPCSS do internetu. Internetová konektivita je primárně realizována připojením do dvou nezávislých uzlů NIX dvěma nezávislými optickými trasami o kapacitě 10 Gbps a sekundárně připojením dvěma nezávislými linkami 100 Mbps přes ISP;

- připojení řešení z datových center SPCSS do GOVBONE. Připojení je zajištěno redundantními propoji v rámci DC SPCSS;
- propojení datových center DC Vápenka a DC Zeleneč – DCI;
- firewall a IPS;
- aplikační firewall a loadbalancer F5;
- VPN – vzdálené připojení do sítě SPCSS pomocí VPN, a to buď jako site-to-site VPN nebo remote-access VPN. Určeno pro dodavatele pro účely vzdálené správy aplikace.

Součástí výše uvedených položek je následující podpůrná infrastruktura a související služby, které jsou nezbytné pro provoz bezpečného propojení:

- plně redundantní síťová infrastruktura Poskytovatele;
- ochrana proti DoS a DdoS útokům;
- přiřazení a aktualizace bezpečnostních oprávnění uživatelům a zařízením v síti;
- aktualizace a opravy prvků síťové infrastruktury;
- vyhodnocování a optimalizace výkonu sítě a síťových prvků;
- zajištění dokumentace poskytovaných služeb a jejich technického nastavení pro potřeby Objednatele v takovém rozsahu, aby Objednatel byl schopen dokumentovat správu a provoz aplikační vrstvy ve všech provozních stavech podporovaných aplikací;
- řízení provozu a dohled nad kvalitou poskytované služby;
- řízení provozu a dohledu nad kvalitou poskytované služby vychází z požadavků příslušných standardů ITIL a norem ČSN ISO/IEC 20000.

2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb

2.4.1 Řízení provozu Systému zahrnuje zejména:

- koordinaci provozu HW a SW;
- řízení v oblasti rizik a kvality;
- řízení komunikace mezi dodavatelem aplikace a poskytovatelem;
- koordinaci změnových řízení v rámci poskytování služby.

2.4.2 Podpora poskytování služby prostřednictvím SW nástrojů SPCSS zahrnuje zejména:

- poskytování informací pro posouzení postupu řešení nedostupnosti a závad služby;
- procesní řízení získaných informací;
- SW a personální zajištění.

2.4.3 Dohled nad kvalitou poskytované služby zahrnuje zejména:

- trvalý provozní a bezpečnostní dohled;
- vyhodnocování SLA specifikované v Katalogovém listu.

Infrastruktura SPCSS splňuje veškeré požadavky na provozování OpenData který poskytuje podporu Službě MF/03 – provoz informačních portálů, který je klasifikovaný jako významný informační systém dle zákona č. 181/2014 Sb. O kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), včetně dalších požadavků prováděcích předpisů a nařízení. SPCSS je ve vztahu k MF významným dodavatelem IS OpenData.

Bezpečnost a dohledy na úrovni infrastruktury obsahuje bezpečnostní a provozní dohled na úrovni odpovídající charakteru části služby:

- poskytování výpočetního výkonu;
- poskytování správy operačních systémů;
- poskytování správy databází;
- zajišťování provozu bezpečného komunikačního rozhraní.

Výstupy z bezpečnostního monitoringu jsou integrální součástí zprávy o stavu bezpečnosti infrastruktury k MF/03.

Poskytovatel se zavazuje tímto plnit povinnosti, které vychází ze shora uvedené legislativy.

Poskytovatel je povinen při poskytování infrastrukturních služeb plně implementovat a provádět ustanovení ZoKB a VoKB, zejména:

- zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury a vést o nich bezpečnostní dokumentaci;
- provádět opatření dle § 11 ZoKB;
- vést veškeré provozní a bezpečnostní záznamy infrastruktury, realizovat organizační a technická opatření požadovaná MF ke sběru a vyhodnocování záznamů dle vyhlášky č. 82/2018 Sb. Vlastními prostředky;
- informovat Manažera kybernetické bezpečnosti MF o zranitelnostech, hrozbách a rizicích a jejich zvládání a pravidelných revizí;
- hlásit Manažeru kybernetické bezpečnosti MF a informovat bezpečnostního správce tohoto systému o bezpečnostních hlášeních, kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech bez zbytečného odkladu;
- hlásit kybernetické bezpečnostní incidenty na Národní úřad pro kybernetickou a informační bezpečnost formou požadovanou VoKB a Manažera kybernetické bezpečnosti MF informovat a hlášení KBI na NÚKIB bez zbytečného odkladu o bezpečnostních incidentech, a to bezodkladně po jejich detekci;
- realizovat bezpečnostní opatření ke zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů po konzultaci s Manažera kybernetické bezpečnosti MF;
- umožnit přístup pro určené osoby Objednatele k řešení tiketů do systému Service Desk Poskytovatele, Manažerovi kybernetické bezpečnosti MF nebo dalším určeným osobám vzdálený přístup k záznamům týkajícím se OpenData v nástroji SIEM;
- komunikovat s MF kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty v rozsahu poskytovaných služeb nebo rozsahu, který by ovlivňoval poskytované služby;
- řídit bezpečnostní rizika OpenData;
- řídit kontinuitu provozu OpenData;
- předávat předem dohodnutou formou data, provozní údaje a informace vyžádané Objednatelem.

3 KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

3.1 Požadovaná měsíční dostupnost oblastí služby

Prostředí	Dostupnost oblastí služby	
	Poskytování výpočetního výkonu a zálohovacích kapacit	Zajišťování provozu bezpečného komunikačního rozhraní
Produktivní	99,5 %	99,5 %
Testovací	95,0 %	95,0 %
Vývojové	95,0 %	95,0 %

Nedostupnost služby způsobená hardwarovou nebo jinou technickou závadou infrastruktury některého z prostředí pro provoz OpenData se počítá od okamžiku zahájení nedostupnosti OpenData pro koncové uživatele do okamžiku odstranění této závady. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti OpenData pro koncové uživatele, počítá se nedostupnost služby od doby jejího nahlášení do Service Desku SPCSS.

Za **nahlášení nedostupnosti služby** se považuje založení odpovídajícího servisního hlášení v aplikaci **Service Desk SPCSS** (servicedesk.spcss.cz).

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 \times \frac{T - N}{T}$$

kde

D je dostupnost [%] v daném období.

T vyjadřuje fond provozní doby služby v daném období.

N vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky schválené mimořádné odstávky.

Servisní okna poskytované služby jsou ve čtvrtek od 20:00 do 6:00 a pokud budou mít činnosti v servisním okně dopad do dostupnosti, bude Poskytovatel žádat o jejich schválení formou mimořádné odstávky.

3.2 Požadované lhůty pro obnovení služby

Prostředí	Lhůta pro obnovení služby v běžné provozní době v hodinách		
	Incident kategorie A	Incident kategorie B	Incident kategorie C
Produktivní	4	6	24
Vývojové	24	72	168
Testovací	24	72	168

Kategorizace incidentů:

Incident kategorie A	Služba není použitelná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje jeho užívání většině nebo všem jejím uživatelům. Tento stav kritickým způsobem ohrožuje běžný provoz Objednatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody, a při tom neexistuje náhradní způsob zajištění poskytování služeb tohoto systému.
Incident kategorie B	Služba, je ve svých funkcích degradován tak, že tento stav zásadně omezuje běžný provoz Objednatele.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

3.3 Požadované lhůty pro obnovení služby pro vybrané komponenty

Lhůty pro obnovení služby v produktivním prostředí provozovaném v době konání plánovaného a odsouhlaseného Disaster Recovery testu (komponenty služby 2.1 Poskytování výpočetního výkonu a zálohování a 2.3 zajišťování provozu bezpečného komunikačního rozhraní) jsou stejné jako v testovacím prostředí, tedy:

Prostředí	Lhůta pro obnovení služby v běžné provozní době v době konání plánovaného a odsouhlaseného Disaster Recovery testu		
	Incident kategorie A	Incident kategorie B	Incident kategorie C
Produktivní	24	72	168

4 CENA SLUŽBY

Rozdělení služby dle odst. 2 tohoto katalogového listu	Měsíční cena v Kč (MF/09)		
	bez DPH	DPH	s DPH
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	2 999,00	629,79	3 628,79
2.2 Poskytování správy, servisní podpory SW a údržby HW (Provozní služba)	10 350,00	2 173,50	12 523,50
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	15 927,00	3 344,67	19 271,67
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	16 498,00	3 464,58	19 962,58
Celková měsíční cena	**45 774,00**	**9 612,54**	**55 386,54**

5 SMLUVNÍ POKUTY ZA NESPLNĚNÍ KVALITATIVNÍCH PARAMETRŮ POSKYTOVÁNÍ SLUŽBY

Za porušení kvalitativních parametrů, nedodržení dostupnosti služby dle pododst. 3.1 a nedodržení požadované lhůty pro obnovení služby dle pododst. 3.2 a pododst. 3.3, je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu vypočítanou za jednotlivé oblasti služby dle odst. 2 tohoto katalogového listu.

Název parametru	Smluvní pokuta za porušení parametru služby v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Max. výše smluvní pokuty v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Způsob výpočtu
Dostupnost oblasti Služby	1	40	za každých započatých 15 minut nad povolený limit nedostupnosti nebo doby vyřešení incidentu
Doba vyřešení incidentu kategorie A	1	40	
Doba vyřešení incidentu kategorie B	0,5	15	
Doba vyřešení incidentu kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období.

Výše smluvní pokuty se při nedodržení dostupnosti konkrétního prostředí nebo nedodržení doby vyřešení incidentu vypočítá jako procento z celkové měsíční ceny služby dle tabulky v odst. 4. tohoto katalogového listu.

MF/10	Housing DWDM

1 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba bude poskytována v režimu nepřetržité služby 24x7 hodin.

2 POPIS ROZSAHU SLUŽBY

Předmětem služby je zajištění nájmu jednoho prostoru pro umístění racku o šířce 800 mm a jednoho racku o šířce 800 mm v datovém centru Na Vápence pro instalaci technických a telekomunikačních zařízení Objednatele.

Oblast – Infra služba

2.1 Housing dvou racků

SPCSS jako Poskytovatel služeb zajistí poskytnutí prostoru 1 ks stojanu (racku) šíře 800 mm a 1 ks prostoru včetně racku pro instalaci technických a telekomunikačních zařízení Objednatele v prostorách Datového centra.

Poskytovatel zajistí provoz kritické infrastruktury datového centra pro zajištění zálohovaného napájení a chlazení instalovaných technických zařízení Objednatele. Garantovaný příkon pro prostor pro umístění technických zařízení a pro pronájem Racku je podle požadavku objednatele 6 kW. Poskytovatel bude v rámci dohledového centra zajišťovat kontrolu a dohled zálohovaného napájení a chlazení.

Poskytovatel zajistí, že pro odběr zálohované elektrické energie pro dané instalované technické a telekomunikační zařízení, bude připraveno redundantní napájení. Objednatel zajistí instalaci připojení svých technických a telekomunikačních zařízení k odběru zálohované elektrické energie podle požadavků Poskytovatele.

Poskytovatel měří a kontroluje spotřebu zálohované elektrické energie vždy k poslednímu dni uplynulého kalendářního měsíce.

Objednatel se zavazuje dodržovat požadavky Poskytovatele při instalaci připojení k odběru zálohované elektrické energie. Poskytovatel zajistí kontrolu připojení technických a telekomunikačních instalovaných zařízení v souladu s interními předpisy Poskytovatele. Objednatel se zavazuje umístit do jednoho Racku jen tolik zařízení, aby součet jejich příkonů v zapnutém stavu a při plném výkonu nepřekročil garantovaný příkon na Rack.

Poskytovatel současně průběžně sleduje okamžitý příkon zálohované energie. Pokud tento příkon překročí smluvně sjednanou hodnotu garantovaného o více než 5 % nebo déle než 5 minut, je Poskytovatel oprávněn kontaktovat telefonicky oprávněné osoby Objednatele a současně prokazatelně písemně (doručením do datové schránky) sdělit tuto skutečnost Objednateli. Pokud Objednatel nezjedná nápravu do 3 dnů od doručení tohoto písemného oznámení, má Poskytovatel právo:

- odpojit Rack, aby nedošlo k překročení kritického příkonu zálohované energie pro datový sál;
- odpojit Rack, aby nedošlo k ohrožení chlazení ostatních zařízení umístěných v datovém sále;
- automaticky odpojit Rack, jehož okamžitý příkon dosáhl jmenovitou hodnotu příkonu jističe Racku.

V prostorách Poskytovatele není možné umístit pouze telekomunikační zařízení, která budou narušovat provozní podmínky v datovém centru Poskytovatele a ovlivňovat ostatní zde umístěné technologie (například silné vysílače elektromagnetického vlnění, extrémně hlučná zařízení, zařízení ovlivňující extrémním způsobem teplotu, vlhkost nebo prašnost okolí).

2.2 Zajišťování objektové bezpečnosti a řízeného přístupu

Objektová bezpečnost je zajištěna pomocí Systému komplexního zabezpečení objektů Poskytovatele (dále jen „SKZO").

Autorizace vstupu fyzických osob do objektu Poskytovatele je realizována personální propustí. Autorizace vstupu oprávněných osob do oblastí na úrovni datových sálů je realizována prostřednictvím elektronické kontroly přístupu osob.

Součástí SKZO v jednotlivých datových sálech je vedle plášťové a prostorové technické ochrany i předmětová ochrana HW prostředků – Racku. Objednatel proto umožní Poskytovateli instalaci čidel MAM do umístěného Racku (k zajištění identifikace jeho otevření) pro realizaci napojení do SKZO.

Poskytovatel v rámci řízeného přístupu rovněž zajistí:

- sledování vstupů fyzických osob do prostor datového centra;
- sledování vstupů oprávněných osob do datového sálu, ve kterém je poskytována služba;
- sledování otevření umístěného Racku, který je součástí poskytované služby;
- sledování vstupů členů servisních organizací Objednatele, kteří budou oprávnění ke vstupu do datového sálu.

2.3 Zajištění non-IT dohledu

Poskytovatel v rámci dohledu kritické infrastruktury zajistí:

- sledování hodnot teploty v datovém sále, ve kterém je poskytovaná služba;
- sledování hodnot vlhkosti v datovém sále, ve kterém je poskytovaná služba;
- průběžné sledování okamžitého příkonu zálohované energie pro napájení umístěného Racku Objednatele;
- sledování Elektronického požárního systému (dále jen „EPS“).

Poskytovatel nezajišťuje dohled konektivity připojení poskytnutých prostorů pro technická zařízení k zařízení telekomunikačního operátora Objednatele.

Poskytovatel se zavazuje udržovat teplotu v datovém sále v úrovni 22 °C (s tolerancí +-3 °C). Služba je považována za nedodanou, pokud teplota dosáhne 25,1 °C a více anebo není zajištěno napájení každého pronajatého racku ani z jedné fáze. Služby jsou považovány za dodané, pokud je zajištěno napájení předmětných technologií alespoň z jedné fáze a současně teplota není vyšší než 25,0 °C.

Komunikace mezi Poskytovatelem a Objednatelem při upozornění a při poskytování informací z non-IT dohledu bude realizována formou telefonických hovorů a mailem.

Informace o non-IT dohledu budou součástí Zprávy o úrovni a rozsahu poskytovaných služeb v období.

Poskytovatel poskytne Objednatelem vyžádanou provozní podporu při odstávkách jeho technických a telekomunikačních zařízení umístěných v datových centrech.

Oblast – ZNaCh

2.4 Služba zálohovaného napájení a chlazení

Objednatel se zavazuje hradit Poskytovateli cenu za skutečně spotřebovanou elektrickou energii za zálohované napájení a chlazení podle odst. 6.3 Smlouvy.

3 KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

3.1 Požadovaná měsíční dostupnost oblastí služby

Požadovaná měsíční dostupnost služby	99,982 %

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 \times \frac{T - N}{T}$$

kde

D je dostupnost [%] v daném období.

T vyjadřuje fond provozní doby služby v daném období.

N vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky schválené mimořádné odstávky.

4 CENA SLUŽBY

Rozdělení služby dle odst. 2 tohoto katalogového listu	Měsíční cena v Kč (MF/10)		
	bez DPH	DPH	s DPH
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Housing (Infra služba)	55 169,00	11 585,49	66 754,49
2.4 Služba zálohovaného napájení a chlazení (ZNaCh)	Cena za ZNaCh bude vypočtena jako součin celkové měsíční spotřeby elektrické energie v kWh měřené na vstupech do racků a ceny za 1kWh ZNaCh. Cena ZNaCh je stanovena jako součin měsíční fakturované ceny dodavatele el. energie a příslušného parametru efektivity využití elektrické energie v datovém centru Poskytovatele – tzv. PUE. Vyúčtování ceny proběhne dle čl. VI odst. 6.3 Smlouvy.		

5 SMLUVNÍ POKUTY ZA NESPLNĚNÍ KVALITATIVNÍCH PARAMETRŮ POSKYTOVÁNÍ SLUŽBY

Za porušení kvalitativních parametrů, nedodržení dostupnosti služby dle pododst. 3.1 je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu vypočítanou za jednotlivé podslužby dle odst. 2 tohoto katalogového listu.

Název parametru	Smluvní pokuta za porušení parametru služby v % z celkové měsíční ceny služby včetně	Max. výše smluvní pokuty v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Způsob výpočtu

	DPH dle odst. 4 tohoto KL		
Dostupnost služby housing	1	40	za každých započatých 15 minut nad povolený limit nedostupnosti nebo doby vyřešení incidentu

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období.

Výše smluvní pokuty se při nedodržení dostupnosti konkrétní služby vypočítaná jako procento z celkové měsíční ceny služby dle tabulky v odst. 4. tohoto katalogového listu.

MF/011	Zajištění a provoz prostředí pro IS FORM

1 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba bude poskytována pro prostředí IS FORM v režimu 24x7 hodin. Služba bude poskytovaná v rámci on-premise datových center SPCSS.

Prostředí pro testování bude poskytováno pouze v režimu 8x5 hodin ve zkrácené provozní době, tj. v pracovních dnech od 8:00 do 16:00 hod.

2 POPIS ROZSAHU SLUŽBY

Obsahem služby Zajištění a provoz prostředí pro IS FORM v režimu podle čl. 1 tohoto Katalogového listu je zajištění bezpečného a spolehlivého provozu tohoto prostředí. V termínu zahájení poskytování služby Zajištění a provoz prostředí pro IS FORM podle tohoto katalogového listu má MF k dispozici HW a SW infrastrukturu uvedeného prostředí pro provoz IS FORM. Detailní HW a SW specifikace je popsána v jednotlivých oblastech služby.

Oblast – Infra služby

2.1 Poskytování výpočetního výkonu

Služba bude realizována prostřednictvím zdrojů výpočetního výkonu na platformě MS Azure Stack Hub (dále jen „AzS"), které má dostatečný výpočetní výkon, pro provozování IS FORM a požadovanou dostupnost.

Architektura infrastruktury umožňuje pro všechny prvky (servery, storage i komunikace) standardní škálování vertikálně i horizontálně s minimálním dopadem na provoz.

2.1.1 Výpočetní výkon na platformě MS Azure Stack Hub

Poskytování výpočetního výkonu na platformě MS Azure Stack (dále také „AzS") je realizováno prostřednictvím alokace zdrojů a kapacity v rámci AzS provozovaného Poskytovatelem pro požadovaný počet serverů s operačními systémy Windows nebo Linux. Objednatel díky Službě bude mít možnost komunikace z a do prostředí AzS Poskytovatele.

Platforma AzS funguje jako prostředí hyperkonvergované infrastruktury provozované v datových centrech Poskytovatele. Jako hlavní škálovatelná jednotka výpočetního výkonu je v prostředí AzS nabízen virtuální server v podobě plánu, kde každý takový plán má předem stanovenou výši parametrů virtualizovaného výpočetního výkonu (vCPU) a virtualizované RAM.

Pro účely provozu a využití platformy AzS budou pro Objednatele vytvořeny a zpřístupněny administrátory Poskytovatele následující zdroje dle požadavku Objednatele.

2.1.2 Celkové výkonnostní parametry všech prostředí on-premise IS FORM jsou uvedeny v následující tabulce:

Službě přiřazené HW virtualizované prostředky (úvodní konfigurace)	Plán v AzureStacku	Počet kusů
Produktivní prostředí		
Aplikační server pro produkční prostředí s OS RHEL 8 vCPU, 16 GB vRAM, 64 GB vHDD	AZS_C1_8_16	1
Databázový server pro produkční prostředí s OS WIN 8 vCPU, 28 GB vRAM, 128 GB vHDD a 256 GB vHDD	AZS_C2_8_28	1
Testovací prostředí		
Aplikační server pro produkční prostředí s OS RHEL 8 vCPU, 16 GB vRAM, 64 GB vHDD	AZS_C1_8_16	1
Databázový server pro produkční prostředí s OS WIN 4 vCPU, 14 GB vRAM, 128 GB vHDD a 256 GB vHDD	AZS_B2_4_14	1

Celkový poskytovaný výkon pro jednotlivá prostředí bude Poskytovatel vykazovat v pravidelných měsíčních Zprávách o rozsahu a úrovni poskytované služby. Výpočetní výkon a diskový prostor, resp. jejich změny, budou realizovány na jednotlivých prostředích podle vzájemně schválených změnových požadavků a v dostatečném předstihu prostřednictvím procesů stanovených v rámci struktury řízení provozu (viz. Příloha č.3 Smlouvy).

2.1.3 Poskytování zálohovacích kapacit

Způsob realizace zálohování respektuje požadavky na dostupnost, výkonnost a umožňuje využít možnosti HW a technologií produkčního prostředí IS FORM, zejména diskových polí a páskových knihoven. Zálohovací systém realizuje zálohování stanoveným způsobem a režimem nutným k zajištění SLA. Standardem je zálohování operačních systémů, vybraných souborových systémů a databází.

Požadavky na RPO, RTO a zálohovací plány jsou uvedeny v provozní dokumentaci a jsou schvalovány řídícími orgány provozu.

Oblast – Provozní služby

2.2 Poskytování správy, servisní podpory SW a údržby HW

2.2.1 Poskytování správy operačních systémů

Služba je poskytována na následujících operačních systémech:

- MS Windows: MS Windows Server Datacenter 2022 a vyšší;
- RedHat 9.0 a vyšší.

Předpokladem služby pro licencované operační systémy je zajištění licence a maintenance OS – licence OS zajistí Poskytovatel.

Součástí služby není implementace a správa aplikačních komponent operačních systémů, respektive aplikačního SW přibaleného k základnímu OS, jako jsou například web servery, aplikační servery, middleware, nebo adresářové služby pro účely správy aplikačních uživatelů.

Služba zahrnuje následující činnosti:

- administrace operačních systémů, tzn. incident management, problem management a change management (vyjma změn aplikačních komponent – viz. výše);
- aktualizace operačních systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost aplikací;
- kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;

- provádění restartů operačních systémů dle požadavků Objednatele;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- součinnosti s případnou instalací a konfigurací nového software;
- instalace a údržba certifikátů doporučených dodavatelem aplikace pro zabezpečení přístupů na servery;
- úpravy výkonnostních parametrů systému;
- správa souborového systému (filesystem, přístupová práva a zaplněnost);
- testování změn provedených v OS;
- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);
- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele probíhá formou nástrojů typu sudo nebo jsou řízeny pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;
- Poskytovatel instaluje vždy minimální výchozí instalaci operačního systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace (balíčky, filesystemy, úpravy v konfiguračních souborech).

2.2.2 Poskytování správy databází

Služba je poskytována na následujících verzích databázového systému:

- MS SQL Standard 2022.

Předpokladem služby pro licencované databázové systémy je zajištění licence a její maintenance – potřebné licence databázového systému MS SQL Standard zajišťuje Objednatel.

Služba zahrnuje následující činnosti:

- administrace databázových systémů, tzn. incident management, problem management a change management;
- aktualizace databázových systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a doporučení bezpečnostních autorit s ohledem na stabilitu provozu, bezpečnost a dostupnost databází;
- pravidelný monitoring výkonových charakteristik, vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu), proaktivní návrh opatření a změn v nastavení infrastruktury a provozovaných SW komponent vyplývajících z nálezů a analýzy monitoringu prostředí;
- úpravy výkonnostních parametrů databáze;
- testování změn provedených v databázi;
- pravidelné testování chování v obvyklých provozních režimech (např. DR testy);
- součinnost při testování aplikací (např. aplikační nebo zátěžové testy aplikací);
- součinnost při řešení problémů aplikací.

Předpokladem poskytování služeb je splnění následujících pravidel:

- účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele jsou řízeny pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele;

- Poskytovatel instaluje vždy minimální výchozí instalaci databázového systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném databázovém systému provést nad rámec minimální instalace.

2.3 Zajišťování provozu bezpečného komunikačního rozhraní

V rámci zajišťování provozu bezpečného komunikačního rozhraní jsou typicky čerpány následující podslužby:

- připojení řešení z datových center SPCSS do internetu. Internetová konektivita je primárně realizována připojením do dvou nezávislých uzlů NIX dvěma nezávislými optickými trasami o kapacitě 10 Gbps a sekundárně připojením dvěma nezávislými linkami 100 Mbps přes ISP;
- připojení řešení z datových center SPCSS do GOVBONE a CMS2. Připojení je zajištěno redundantními propoji v rámci DC SPCSS;
- propojení datových center DC Vápenka a DC Zeleneč – DCI;
- firewall a IPS;
- aplikační firewall a loadbalancer F5;
- VPN – vzdálené připojení do sítě SPCSS pomocí VPN, a to buď jako site-to-site VPN nebo remote-access VPN. Určeno pro dodavatele pro účely vzdálené správy aplikace.

  Součástí výše uvedených položek je následující podpůrná infrastruktura a související služby, které jsou nezbytné pro provoz bezpečného propojení:
- plně redundantní síťová infrastruktura Poskytovatele;
- ochrana proti DoS a DDoS útokům;
- přiřazení a aktualizace bezpečnostních oprávnění uživatelům a zařízením v síti;
- aktualizace a opravy prvků síťové infrastruktury;
- vyhodnocování a optimalizace výkonu sítě a síťových prvků;
- zajištění dokumentace poskytovaných služeb a jejich technického nastavení pro potřeby Objednatele v takovém rozsahu, aby Objednatel byl schopen dokumentovat správu a provoz aplikační vrstvy ve všech provozních stavech podporovaných aplikací;
- řízení provozu a dohled nad kvalitou poskytované služby;
- řízení provozu a dohledu nad kvalitou poskytované služby vychází z požadavků příslušných standardů ITIL a norem ČSN ISO/IEC 20000.

Služby zajištění provozu bezpečného komunikačního rozhraní		
Popis	**Počet jednotek**	**Jednotka**
Internet – peering NIX	1,00	Mbps
Stavový firewall	2,00	Mbps
VPN	8,00	VPN

2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb

2.4.1 Řízení provozu Systému zahrnuje zejména:

- koordinaci provozu HW a SW;
- řízení v oblasti rizik a kvality;
- řízení komunikace mezi dodavatelem aplikace a poskytovatelem;
- koordinaci změnových řízení v rámci poskytování služby.

2.4.2 Podpora poskytování služby prostřednictvím SW nástrojů SPCSS zahrnuje zejména:

- poskytování informací pro posouzení postupu řešení nedostupnosti a závad služby;
- procesní řízení získaných informací;
- SW a personální zajištění.

2.4.3 Dohled nad kvalitou poskytované služby zahrnuje zejména:

- trvalý provozní a bezpečnostní dohled;
- vyhodnocování SLA specifikované v Katalogovém listu.

Poskytování služby Zajištění a provoz produkčního prostředí pro IS FORM musí splňovat veškeré požadavky na Významný informační systém dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), včetně dalších požadavků prováděcích předpisů a nařízení, zejména Směrnice SŘBI MF. SPCSS je ve vztahu k MF významným dodavatelem a provozovatelem IS FORM.

Bezpečnost a dohledy na úrovni infrastruktury obsahuje bezpečnostní a provozní dohled na úrovni odpovídající charakteru části služby:

- poskytování výpočetního výkonu;
- poskytování správy operačních systémů;
- poskytování správy databází
- zajišťování provozu bezpečného komunikačního rozhraní.

Pravidelným měsíčním výstupem bezpečnostního dohledu je zpracování Zprávy o stavu bezpečnosti infrastruktury, která je součástí Zprávy.

Poskytovatel se zavazuje tímto plnit povinnosti, které vychází ze shora uvedené legislativy.

Poskytovatel je povinen při poskytování infrastrukturních služeb plně implementovat a provádět ustanovení ZoKB a VoKB, zejména:

- zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury a vést o nich bezpečnostní dokumentaci;
- provádět opatření dle § 11 ZoKB;

- vést veškeré provozní a bezpečnostní záznamy infrastruktury, realizovat organizační a technická opatření požadovaná MF ke sběru a vyhodnocování záznamů dle vyhlášky č. 82/2018 Sb. vlastními prostředky;
- informovat Manažera kybernetické bezpečnosti MF o zranitelnostech, hrozbách a rizicích a jejich zvládání a pravidelných revizí;
- hlásit Manažeru kybernetické bezpečnosti MF a informovat bezpečnostního správce tohoto systému o bezpečnostních hlášeních, kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech bez zbytečného odkladu;
- hlásit kybernetické bezpečnostní incidenty na Národní úřad pro kybernetickou a informační bezpečnost formou požadovanou VoKB a Manažera kybernetické bezpečnosti MF informovat a hlášení KBI na NÚKIB bez zbytečného odkladu o bezpečnostních incidentech, a to bezodkladně po jejich detekci;
- realizovat bezpečnostní opatření ke zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů po konzultaci s Manažera kybernetické bezpečnosti MF;
- umožnit přístup pro určené osoby Objednatele k řešení tiketů do systému Service Desk Poskytovatele, Manažerovi kybernetické bezpečnosti MF nebo dalším určeným osobám vzdálený přístup k záznamům týkajícím se IS FORM v nástroji SIEM;
- komunikovat s MF kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty v rozsahu poskytovaných služeb nebo rozsahu, který by ovlivňoval poskytované služby;
- řídit bezpečnostní rizika IS FORM;
- řídit kontinuitu provozu IS FORM;
- předávat předem dohodnutou formou data, provozní údaje a informace vyžádané Objednatelem;

3 KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

3.1 Požadovaná měsíční dostupnost oblastí služby

Prostředí	Dostupnost oblastí služby	
	Poskytování výpočetního výkonu a zálohovacích kapacit	**Zajišťování provozu bezpečného komunikačního rozhraní**
Produktivní	99,5 %	99,5 %
Testovací	95,0 %	95,0 %

Nedostupnost služby způsobená hardwarovou nebo jinou technickou závadou infrastruktury některého z prostředí pro provoz IS FORM se počítá od okamžiku zahájení nedostupnosti IS FORM pro koncové uživatele do okamžiku odstranění této závady. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti IS FORM pro koncové uživatele, počítá se nedostupnost služby od doby jejího nahlášení do Service Desku SPCSS.

Nedostupnost služby způsobená softwarovou závadou infrastruktury IS FORM (nastavení systému, pravidla a prostupy firewalu, apod.) se počítá od okamžiku nahlášení nedostupnosti IS FORM pro koncové uživatele do okamžiku odstranění této závady.

Za **nahlášení nedostupnosti služby** se považuje založení odpovídajícího servisního hlášení v aplikaci **Service Desk SPCSS** (servicedesk.spcss.cz).

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 \times \frac{T - N}{T}$$

kde

D je dostupnost [%] v daném období

T vyjadřuje fond provozní doby služby v daném období

N vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky schválené mimořádné odstávky.

Servisní okna poskytované služby jsou v době plánované odstávky, zveřejněné vždy předem ve formě Plánu odstávek na kalendářní rok, případně ve čtvrtek od 20:00 do 6:00 vyjma čtvrtka před plánovanou odstávkou. Pokud budou mít činnosti v servisním okně dopad do dostupnosti, bude Poskytovatel žádat o jejich schválení formou mimořádné odstávky.

3.2 Požadované lhůty pro obnovení služby

Prostředí	Lhůta pro obnovení služby v běžné provozní době v hodinách		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Produktivní	4	8	55
Testovací	24	72	168

Kategorizace incidentů:

Incident kategorie A	Služba není použitelná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje jeho užívání většině nebo všem jejím uživatelům. Tento stav kritickým způsobem ohrožuje běžný provoz Objednatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody, a při tom neexistuje náhradní způsob zajištění poskytování služeb tohoto systému.
Incident kategorie B	Služba, je ve svých funkcích degradován tak, že tento stav zásadně omezuje běžný provoz Objednatele.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

3.3 Požadované lhůty pro obnovení služby pro vybrané komponenty

Lhůty pro obnovení služby v produktivním prostředí provozovaném v době konání plánovaného a odsouhlaseného Disaster Recovery testu (komponenty služby 2.1 Poskytování výpočetního výkonu a zálohování a 2.3 zajišťování provozu bezpečného komunikačního rozhraní) jsou stejné jako v testovacím prostředí, tedy:

Prostředí	Lhůta pro obnovení služby v běžné provozní době v době konání plánovaného a odsouhlaseného Disaster Recovery testu		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Produktivní	24	72	168

4 CENA ZA SLUŽBU

Měsíční cena za jednotlivé oblasti služby:

Rozdělení služby dle odst. 2 tohoto katalogového listu	Měsíční cena v Kč (MF/11)		
	bez DPH	DPH	s DPH
Měsíční cena v období od 01.04.2025 do 31.03.2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	27 720,00	5 821,20	33 541,20
2.2 Poskytování správy, servisní podpory SW a údržby HW (Provozní služba)	-	-	-
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	9 030,00	1 896,30	10 926,30
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	4 128,00	866,88	4 994,88
Celková měsíční cena	**40 878,00**	**8 584,38**	**49 462,38**

5 SMLUVNÍ POKUTY ZA NESPLNĚNÍ KVALITATIVNÍCH PARAMETRŮ POSKYTOVÁNÍ SLUŽBY

Za porušení kvalitativních parametrů, nedodržení dostupnosti služby dle pododst. 3.1 a nedodržení požadované lhůty pro obnovení služby dle pododst. 3.2 a pododst. 3.3, je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu vypočítanou za jednotlivé oblasti služby dle odst. 2 tohoto katalogového listu.

Název parametru	Smluvní pokuta za porušení parametru služby v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Max. výše smluvní pokuty v % z celkové měsíční ceny služby včetně DPH dle odst. 4 tohoto KL	Způsob výpočtu
Dostupnost oblasti Služby	1	40	za každých započatých 15 minut nad povolený limit nedostupnosti nebo doby vyřešení incidentu
Doba vyřešení incidentu kategorie A	1	40	
Doba vyřešení incidentu kategorie B	0,5	15	
Doba vyřešení incidentu kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období.

Výše smluvní pokuty se při nedodržení dostupnosti konkrétního prostředí nebo nedodržení doby vyřešení incidentu vypočítá jako procento z celkové měsíční ceny služby dle tabulky v odst.