Číslo Smlouvy MF
23/906/0039
Toto číslo uvádějte při fakturaci

SMLOUVA 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

(dále jen „**Smlouva**")

Česká republika – Ministerstvo financí
se sídlem: Letenská 525/15, 118 10 Praha 1
za niž jedná: xxx
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: xxx
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 jednotlivě též jen „**Smluvní strana**" nebo společně „**Smluvní strany**")

uzavírají v souladu s ustanovením § 1746 odst. 2 a násl. a s přihlédnutím k § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**OZ**"), a příslušnými ustanoveními zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**") tuto

Smlouvu

I. ÚVODNÍ USTANOVENÍ

1.1. Objednatel prohlašuje, že:

1.1.1. je ústředním orgánem státní správy, jehož působnost je stanovena zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů; a

1.1.2. splňuje veškeré podmínky a požadavky ve Smlouvě stanovené a je oprávněn Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.2. Poskytovatel prohlašuje, že:

1.2.1. je státním podnikem existujícím podle českého právního řádu; a

1.2.2. splňuje veškeré podmínky a požadavky ve Smlouvě stanovené a je oprávněn Smlouvu uzavřít a řádně plnit závazky v ní obsažené, a to i jako významný dodavatel ve smyslu 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) (dále jen „**VoKB**").

1.3. Smlouva se uzavírá na základě výjimky z působnosti ZZVZ stanovené v § 11 odst. 1 ZZVZ.

1.4. Pojmy s velkými počátečními písmeny definované ve Smlouvě budou mít význam, jenž je jim ve Smlouvě, včetně jejích příloh a dodatků, přikládán.

1.5. Smluvní strany souhlasí s tím, že označování dokumentů vzniklých na základě této Smlouvy bude probíhat v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.first.org/tlp/).

II. ÚČEL A PŘEDMĚT SMLOUVY

2.1. Účelem této Smlouvy je poskytovat Objednateli služby bezpečného datového centra dle jednotlivých katalogových listů uvedených v Příloze č. 1 až Příloze č. 3 Smlouvy, a to dle specifikace a v rozsahu uvedeném vždy v dané příloze Smlouvy (resp. její části) (to vše dále jen „**Služby**").

2.2. Předmětem této Smlouvy je závazek Poskytovatele zajistit pro Objednatele poskytování zejména následujících oblastí Služeb:

2.2.1. služby poskytování infrastruktury, např. výpočetní výkon, zálohování (dále jen „**Infra služby**");

2.2.2. zálohované napájení a chlazení (dále jen „**ZNaCh**");

2.2.3. provozní služby informačních systémů související s jednotlivými informačními systémy Objednatele, např. provozní dohled infrastruktury, bezpečnostní dohled, řízení služeb infrastruktury (to vše dále jen „**Provozní služby**");

2.2.4. cloudové služby, tj. provoz služeb infrastruktury komerčních poskytovatelů založených na standardních jednotkách dle aktuálních nabídek komerčních poskytovatelů, v rámci kterých, se Poskytovatel zavazuje poskytovat přípravu, provoz a ukončení služeb infrastruktury komerčních poskytovatelů (dále jen „**Cloudové služby**");

2.2.5. odborné role za účelem implementačních a podpůrných provozních činností mimo rozsah Infra služeb a Provozních služeb, přičemž jde o činnosti související s poskytováním infrastruktury a provozních služeb dle této Smlouvy a jsou poskytovány dle jednotlivých rolí uvedených v katalogu rolí, který je součástí Přílohy č. 2 Smlouvy (dále jen „**Poskytování odborných rolí**");

2.2.6. specifické služby kybernetické bezpečnosti, tj. služby v oblasti kybernetické bezpečnosti, které jsou poskytovány pro konkrétní aplikace Objednatele na základě písemného požadavku Oprávněné osoby Objednatele (dále jen „**Specifické služby KB**"). Konkrétní definice dané Specifické služby KB na vyžádání bude vytvořena Poskytovatelem na základě analýzy požadavků Objednatele s využitím především popisu služeb kybernetické bezpečnosti uvedeném v Příloze č. 3 Smlouvy, kdy výstupem předmětné analýzy bude nový katalogový list, který bude formou změnového řízení postupem dle Smlouvy a následným uzavřením dodatku ke Smlouvě zařazen do katalogu služeb v Příloze č. 1 Smlouvy. Předmětná služba bude následně poskytována v souladu s postupem, který bude případně stanoven předmětným dodatkem ke Smlouvě. Pro vyloučení pochybností Smluvní strany uvádějí, že běžné provozní služby v oblasti kybernetické bezpečnosti pro infrastrukturní služby jsou zahrnuty do Služeb popsaných v jednotlivých katalogových listech v Příloze č. 1 Smlouvy;

přičemž specifikace poskytovaných Služeb vč. parametrů Služeb ve výše uvedeném členění je uvedena vždy v Příloze č. 1 (kdy dle příslušného Katalogového listu mohou být poskytovány všechny Služby dle pododst. 2.2.1 až 2.2.4 či pouze některé z nich) a Příloze č. 2 a Příloze č. 3 Smlouvy (kde jsou blíže specifikovány Poskytování odborných rolí a Specifické služby KB). Předmětem Smlouvy je dále závazek Objednatele zaplatit Poskytovateli za řádné poskytnutí Služeb cenu dle čl. VI této Smlouvy.

2.3. Pro vyloučení pochybností Smluvní strany uvádějí, že součástí plnění dle Smlouvy mohou být rovněž činnosti přípravy a exitu Služeb, tj. zejména činnosti provozního a dokumentačního charakteru, včetně předávání znalostí, souvisejících s předmětem a rozsahem Služeb dle Smlouvy, přičemž tyto činnosti budou složeny a naceněny dle Služeb uvedených v odst. 2.2 tohoto článku (dále jen „**Exit plán**"). Exit plán bude Poskytovatelem poskytnut pouze na základě požadavku Objednatele, a to prostřednictvím změnového řízení analogicky postupem dle čl. V Smlouvy.

2.4. Objednatel se zavazuje poskytnout Poskytovateli veškerou nezbytnou součinnost potřebnou pro řádné poskytnutí Služeb.

2.5. Poskytovatel prohlašuje, že disponuje veškerými potřebnými odbornými, technickými a právními předpoklady nutnými k realizaci Služeb dle této Smlouvy.

2.6. Smluvní strany berou na vědomí a souhlasí s tím, že v rámci provozu Služeb bude zřízena řídicí struktura provozu Služeb, která je definována v Příloze č. 4 Smlouvy (dále jen „**Řídicí struktura provozu Služeb**"). Smluvní strany se zavazují při plnění Služeb postupovat v souladu s postupy stanovenými v Příloze č. 4 Smlouvy.

2.7. Smluvní strany berou na vědomí, že v rámci plnění Smlouvy dochází ke sběru dat ve smyslu § 22 VoKB, přičemž se jedná o data, která mohou obsahovat osobní údaje, která jsou ve vlastnictví Objednatele jako Správce osobních údajů, a se kterými bude Poskytovatel jako Zpracovatel nakládat pouze dle pokynů Objednatele.

III. MÍSTO A DOBA PLNĚNÍ

3.1. Místem plnění je sídlo Poskytovatele uvedené v záhlaví této Smlouvy, hlavní město Praha a datové centrum Poskytovatele na adrese Čsl. armády 1060, 250 91 Zeleneč (dále jen „**Místo plnění**"), nebude-li Smluvními stranami písemně sjednáno jinak.

3.2. Služby mohou být poskytnuty i vzdáleným přístupem, pokud to povaha plnění dle Smlouvy umožňuje, není-li nezbytné nebo vhodné výkon takového plnění zajistit v Místě plnění (on-site).

3.3. Poskytovatel se zavazuje poskytovat Služby od 1. 4. 2024 po dobu účinnosti Smlouvy (kontinuálně, tj. po dobu trvání stanovenou vždy v příslušném katalogovém listu v Příloze č. 1 či dle požadavku Objednatele, tj. v případě Služeb poskytovaných na požadavek Objednatele, a to vždy dle podmínek stanovených ve Smlouvě pro jednotlivé Služby), a to ve sjednané kvalitě, rozsahu a dle podmínek touto Smlouvou stanovených.

IV. ZPŮSOB A AKCEPTACE PLNĚNÍ

4.1. Poskytovatel se zavazuje poskytovat Služby v kvalitě definované v jednotlivých Service Level Agreements (dále jen „**SLA**"), přičemž SLA jsou specifikovány vždy samostatně v Příloze č. 1 Smlouvy v rámci jednotlivých katalogových listů.

4.2. Poskytnutí Služeb, tj. Infra služeb, ZNaCh, Provozních služeb a Cloudových služeb bude Objednatelem přebíráno na základě potvrzení o poskytnutí Služeb vždy za daný kalendářní měsíc poskytování Služeb a bude realizováno formou podpisu záznamů o poskytnutí Služeb (tj. dle jednotlivých Katalogových listů v Příloze č. 1 Smlouvy) (dále samostatně jen „**Záznam**"), jehož vzor je součástí Přílohy č. 5 Smlouvy, přičemž Poskytovatel vystaví Záznam vždy do 5 pracovních dnů následujících po skončení kalendářního měsíce, ve kterém byly předmětné Služby poskytovány a ve stejné lhůtě jej předloží Oprávněné osobě Objednatele. Objednatel se zavazuje Záznam potvrdit a podepsat ve lhůtě 5 pracovních dnů ode dne doručení Záznamu a ve stejné lhůtě jej doručit Oprávněné osobě Poskytovatele, přičemž v případě, že tak ve stanovené lhůtě neučiní, bude Záznam Poskytovatelem považován za potvrzený. Sporné případy poskytnutí Služeb budou řešeny v rámci Zprávy postupem dle odst. 4.3 tohoto článku.

4.3. Hodnocení a kontrola poskytování Služeb poskytnutých v daném kalendářním měsíci bude probíhat vždy za daný kalendářní měsíc na základě zprávy o úrovni a rozsahu poskytovaných Služeb v příslušném kalendářním měsíci, kterou vyhotoví Poskytovatel a předloží ji Oprávněné osobě Objednatele ve lhůtě 10 pracovních dnů ode dne skončení příslušného kalendářního měsíce, ve kterém byly předmětné Služby poskytovány (dále jen „**Zpráva**"). Vzor Zprávy je součástí Přílohy č. 5 Smlouvy. Objednatel se zavazuje ve lhůtě 5 pracovních dnů ode dne doručení Zprávy tuto Zprávu posoudit, schválit ji a následně doručit Oprávněné osobě Poskytovatele, příp. k neschválené Zprávě ve stejné lhůtě vypracovat písemné stanovisko a předložit ho Oprávněným osobám Poskytovatele. Sporné případy akceptace Služeb budou řešeny do 5 pracovních dnů ode dne doručení stanoviska dle předchozí věty Poskytovateli na jednání Oprávněných osob Smluvních stran, přičemž při naplnění podmínek stanovených touto Smlouvou, tj. při nedodržení stanovených podmínek pro poskytování Služeb Poskytovatelem, je Objednatel oprávněn uplatnit příslušné sankce dle čl. XIII Smlouvy.

4.4. Na základě vyhodnocení Zprávy v příslušném období mohou Oprávněné osoby Smluvních stran navrhnout přijetí případných změn v poskytování Služeb, vč. cenových dopadů, a to formou změnového řízení dle čl. V Smlouvy.

4.5. Realizace Poskytování odborných rolí bude probíhat na základě jednotlivých objednávek uzavíraných vždy do vyčerpání stanoveného finančního limitu či do uplynutí účinnosti objednávky (pro vyloučení pochybností Smluvní strany uvádějí, že účinnost každé Poskytovatelem akceptované objednávky nastane nejdříve jejím zveřejněním v registru smluv v souladu se ZRS, přičemž zveřejnění každé objednávky v registru smluv se zavazuje provést Poskytovatel), podle toho, která ze skutečností nastane dříve (objednávka dále také jen „**Výzva k poskytování odborných rolí**"), a to vždy na základě písemné výzvy Objednatele k poskytnutí Poskytování odborných rolí, která je současně návrhem Výzvy k poskytování odborných rolí, přičemž vzor Výzvy k poskytování odborných rolí je součástí Přílohy č. 5 Smlouvy, zaslané prostřednictvím e-mailové zprávy Oprávněné osobě Poskytovatele. Návrh Výzvy k poskytování odborných rolí musí obsahovat:

4.5.1. identifikační údaje Objednatele a Poskytovatele;

4.5.2. výčet poptávaných rolí a maximální, tj. nepřekročitelnou finanční částku pro čerpání Poskytování odborných rolí na základě příslušné Výzvy k poskytování odborných rolí a uvedení termínu, v rámci kterého má být Poskytnutí odborných rolí provedeno, resp. doby trvání Výzvy k poskytování odborných rolí;

4.5.3. název a popis cílového informačního systému, příp. informačních systémů;

4.5.4. podrobnou specifikaci požadavků na Poskytování odborných rolí dle Katalogu rolí v Příloze č. 2 Smlouvy;

4.5.5. kvalifikovaný elektronický podpis Objednatele.

4.6. Oprávněná osoba Poskytovatele se zavazuje provést potvrzení návrhu Výzvy k poskytování odborných rolí, tj. podepsat Výzvu k poskytování odborných rolí a doručit ji Oprávněné osobě Objednatele ve lhůtě 10 pracovních dnů ode dne doručení návrhu Výzvy k poskytování odborných rolí (dále jen „**Potvrzení** Výzvy k poskytování odborných rolí"), popř. bez zbytečného odkladu požádat Objednatele o doplnění či upřesnění chybějících náležitostí Výzvy k poskytování odborných rolí dle odst. 4.5 tohoto článku. Potvrzením Výzvy k poskytování odborných rolí Poskytovatel vyjadřuje souhlas s obsahem Výzvy k poskytování odborných rolí, a že nepožaduje doplnění či upřesnění chybějících náležitostí a jako takový jej akceptuje. Požádá-li Poskytovatel o doplnění či upřesnění chybějících náležitostí, staví se lhůta pro Potvrzení Výzvy k poskytování odborných rolí do okamžiku zaslání řádně doplněného nového návrhu Výzvy k poskytování odborných rolí. Poskytovatel není oprávněn návrh Výzvy k poskytování odborných rolí jakýmkoliv způsobem doplňovat či měnit a zavazuje se ji potvrdit bez výhrad nebo požádat o doplnění či upřesnění podle tohoto odstavce. Potvrzení Výzvy k poskytování odborných rolí s výhradou se nepovažuje za Potvrzení Výzvy k poskytování odborných rolí ve smyslu tohoto odstavce, není-li ve Smlouvě stanoveno jinak. Doručením písemného podepsaného Potvrzení Výzvy k poskytování odborných rolí Oprávněné osobě Objednatele dochází k uzavření objednávky, tj. Výzvy k poskytování odborných rolí.

4.7. Poskytování odborných rolí bude Objednatelem akceptováno na základě výkazu Poskytování odborných rolí, který se zavazuje Poskytovatel vést v rámci předmětné Výzvy k poskytování odborných rolí (dále jen „**Výkaz**"), jehož vzor je součástí Přílohy č. 5 Smlouvy, a to vždy za daný kalendářní měsíc účinnosti předmětné Výzvy k poskytování odborných rolí. V rámci Výkazu Poskytovatel prokazuje skutečně vynaložený čas na Poskytování odborných rolí detailním popisem jednotlivých činností v rámci jednotlivých rolí v granularitě minimálně po dnech a s přesností vykazovaných objemů činností na celé člověkohodiny. Poskytovatel vystaví Výkaz vždy do 15 kalendářních dnů následujících po skončení kalendářního měsíce, ve kterém bylo Poskytování odborných rolí na základě předmětné Výzvy k poskytování odborných rolí poskytováno a ve stejné lhůtě jej předloží Oprávněné osobě Objednatele ke schválení. Objednatel se zavazuje Výkaz potvrdit a podepsat ve lhůtě 5 pracovních dnů ode dne doručení Výkazu a ve stejné lhůtě jej doručit Oprávněné osobě Poskytovatele, příp. ve stejné lhůtě uvést k Výkazu výhrady a doručit je Poskytovateli Po odstranění veškerých výhrad sepíší Smluvní strany nový Výkaz bez výhrad.

4.8. Současně, aniž by byly dotčeny předcházející odstavce, Smluvní strany sjednávají, že v případě čerpání Cloudových služeb platí následující pravidla:

4.8.1. Poskytování Cloudových služeb bude v režimu TEST a/nebo v režimu VÝVOJ Poskytovatelem poskytováno po dobu účinnosti Smlouvy, resp. po dobu trvání poskytování příslušné Služby dle daného katalogového listu uvedeného v Příloze č. 1 Smlouvy, na základě pokynů Oprávněné osoby Objednatele k zahájení a/nebo k ukončení poskytování Cloudových služeb v režimu TEST a/nebo VÝVOJ a to formou ticketu zadaného prostřednictvím Service Desku Poskytovatele, jak je popsán v Příloze č. 1 Smlouvy (dále jen „**Požadavek k čerpání Cloudových služeb TEST a/nebo VÝVOJ**").

4.8.2. Součástí každého Požadavku k čerpání Cloudových služeb TEST a/nebo VÝVOJ bude vždy specifikace termínu spuštění či termínu ukončení daného prostředí, tj. TEST a/nebo VÝVOJ. Spolu s čerpáním Cloudových služeb v režimu TEST a/nebo VÝVOJ budou vždy čerpány Provozní služby v režimu TEST a/nebo VÝVOJ a dále Služby poskytování infrastruktury v režimu TEST a/nebo VÝVOJ.

4.8.3. Akceptace Cloudových služeb v režimu TEST a/nebo VÝVOJ na základě jednotlivých Požadavků k čerpání Cloudových služeb bude probíhat postupem dle čl. IV odst. 4.2 a 4.3 Smlouvy.

4.9. Řídicí dokumenty vytvořené v souladu s postupy dle Přílohy č. 4 Smlouvy předává Poskytovatel v elektronické podobě ve formátu MS Office.

4.10. Není-li ve Smlouvě ujednáno jinak, Poskytovatel oznámí Objednateli úmysl předat Řídicí dokumenty nejpozději 6 pracovních dnů před zamýšleným dnem předání.

4.11. Objednatel je oprávněn ve lhůtě 4 pracovních dnů od prvního předání Řídicího dokumentu písemně předložit Poskytovateli své připomínky k Řídicímu dokumentu. Poskytovatel vypořádá připomínky Objednatele ve lhůtě 2 pracovních dnů od doručení připomínek Objednatele a předloží Objednateli nový Řídicí dokument. Neakceptuje-li Objednatel nový Řídicí dokument, předá Poskytovateli ve lhůtě 2 pracovních dnů připomínky; Poskytovatel vypořádá připomínky Objednatele z druhého předání připomínek Řídicího dokumentu ve lhůtě 1 pracovního dne a předloží konečnou verzi Řídicího dokumentu způsobem v odst. 4.9 tohoto článku.

4.12. V případě, že Objednatel ve lhůtě 4 pracovních dnů ode dne předání Řídicího dokumentu nepředloží své připomínky, vyzve písemně Poskytovatel Objednatele ke sjednání nápravy a k předložení připomínek ve lhůtě 2 pracovních dnů. Bez obdrženého souhlasu Objednatele s Řídicím dokumentem se tento dokument nepovažuje za akceptovaný.

V. ZMĚNOVÉ ŘÍZENÍ

5.1. Kterákoliv ze Smluvních stran je oprávněna na základě Zprávy písemně navrhnout změny v rozsahu a úrovni poskytovaných Služeb, a to prostřednictvím požadavku zaslaného prostřednictvím e-mailu Oprávněné osobě příslušné Smluvní strany (dále jen „**Změnový požadavek**"). Vzor Změnového požadavku je součástí Přílohy č. 5 Smlouvy. Žádná ze Smluvních stran není povinna navrhované změny akceptovat.

5.2. Poskytovatel se zavazuje provést hodnocení dopadů navrhovaných změn Služeb z hlediska vhodnosti, termínů plnění, součinnosti Smluvních stran a ceny. Poskytovatel se zavazuje provést hodnocení bez zbytečného odkladu, nejpozději do 15 pracovních dnů ode dne doručení Změnového požadavku druhé Smluvní straně, není-li Smluvními stranami dohodnuto jinak.

5.3. Smluvní strany se zavazují za účelem potvrzení změn dle tohoto článku uzavřít dodatek ke Smlouvě, kterým budou provedené změny do Smlouvy promítnuty. V závislosti na takovém dodatku může být upraven požadovaný rozsah plnění Služeb, termíny plnění Služeb, cena Služeb, platební podmínky, součinnost Objednatele atd.

5.4. Změnový požadavek mohou Smluvní strany realizovat výhradně při splnění podmínek stanovených ZZVZ.

VI. CENA A PLATEBNÍ PODMÍNKY

6.1. Smluvní strany se dále dohodly, že za poskytování Infra služeb a Provozních služeb je cena paušální a bude Objednatelem hrazena zpětně po skončení každého kalendářního měsíce poskytování předmětných Služeb a je vždy uvedena (samostatně pro Infra služby a Provozní služby) v předmětném katalogovém listu v Příloze č. 1 Smlouvy (dále jen „**Paušální cena**").

6.2. Smluvní strany se dohodly, že v případě, že Infra služby a/nebo Provozní služby nebudou poskytovány po celý kalendářní měsíc, (tj. v případě, když bude s poskytováním Infra služeb a/nebo Provozních služeb započato v průběhu kalendářního měsíce, případně bude poskytování Infra služeb a/nebo Provozních služeb ukončeno v průběhu kalendářního měsíce), se příslušná Paušální cena poměrně krátí, a to s přesností na celé dny poskytování Infra služeb a/nebo Provozních služeb a Poskytovateli náleží alikvotní část měsíční ceny Infra služeb a/nebo Provozních služeb.

6.3. Objednatel se dále zavazuje hradit Poskytovateli cenu za skutečně spotřebovanou elektrickou energii za ZNaCh (dále jen „**Cena za ZNaCh**"), která bude vypočtena jako součin celkové měsíční spotřeby elektrické energie v kWh měřené na vstupech do racků (bude zjištěno pomocí odečtu vždy k poslednímu dni příslušného kalendářního měsíce) 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. Hodnota PUE Poskytovatele aktuálně činí 1,76. Vždy od 1. 1. daného kalendářního roku Poskytovatel oznámí Objednateli novou hodnotu PUE pro další období následujících 12 kalendářních měsíců na základě výsledků měření tohoto koeficientu za předchozích 12 měsíců, přičemž toto oznámení bude učiněno jednostranně písemnou formou vždy v měsíčním Záznamu bez nutnosti uzavření dodatku ke Smlouvě. K Ceně ZNaCh není Poskytovatelem připočtena žádná režie ani zisk.

6.4. Smluvní strany se dále dohodly, že za Poskytování odborných rolí bude hrazena cena dle jednotlivých rolí, a to za každý člověkoden (tj. 8 člověkohodin) Poskytování odborných rolí ve výši uvedené pro jednotlivé role v Příloze č. 2 Smlouvy (dále jen „**Cena za Poskytování odborných rolí**"). Smluvní strany se dohodly, že v případě neposkytování Poskytování odborných rolí po celý člověkoden se Cena za Poskytování odborných rolí poměrně krátí s přesností na dvě desetinná místa.

6.5. Poskytovatel se zavazuje provádět Cloudové služby za ceny uvedené v Příloze č. 1 Smlouvy (dále jen „**Cena za Cloudové služby**"), přičemž Cena za Cloudové služby je stanovena dle skutečně čerpaného plnění za jeden kalendářní měsíc poskytování Cloudových služeb, je stanovena dohodou Smluvních stran a je stanovena na základě zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů. Cena za Cloudové služby je rovněž stanovena v souladu s principy uvedenými v Příloze č. 1 Smlouvy.

(vše v odst. 6.1, 6.3, 6.4 a 6.5 dále také jednotlivě jen „**Cena za Službu**").

6.6. K Cenám za Službu bude připočítána DPH dle sazby daně ke dni uskutečnění zdanitelného plnění.

6.7. Poskytovatel prohlašuje, že je plátcem DPH.

6.8. Smluvní strany se dohodly, že celkový souhrn plnění v rámci Cloudových služeb dle této Smlouvy, tj. plnění Cloudových služeb po celou dobu účinnosti Smlouvy nesmí přesáhnout částku ve výši 26 400 000 Kč bez DPH (dále jen **„Maximální souhrnná cena za Cloudové služby**"), dále, že celkový souhrn plnění v rámci Poskytování odborných rolí dle této Smlouvy, tj. plnění v rámci všech uzavřených objednávek, resp. Výzev k poskytování odborných rolí nesmí přesáhnout částku ve výši 12 000 000 Kč bez DPH (dále jen **„Maximální souhrnná cena za Poskytování odborných rolí**") a současně, že celkový souhrn plnění v rámci Specifických služeb KB, pokud by byly v budoucnu dle Smlouvy poskytovány v souladu s postupem dle č. II odst. 2.2 pododst. 2.2.6 Smlouvy, tj. plnění Specifických služeb KB po celou dobu účinnosti Smlouvy nesmí přesáhnout částku ve výši 6 000 000 Kč bez DPH (dále jen **„Maximální souhrnná cena za Specifické služby KB**"). Objednatel bere na vědomí a souhlasí s tím, že v případě dosažení Maximální souhrnné ceny za Cloudové služby a/nebo Maximální souhrnné ceny za Poskytování odborných rolí a/nebo Maximální souhrnné ceny za Specifické služby KB (pokud se v budoucnu stanou součástí Smlouvy) nebude Objednatel nadále předmětné Služby dle Smlouvy poskytovat (tj. neuplatní se povinnosti pro poskytování předmětných Služeb dle Smlouvy), a to až do okamžiku případného navýšení uvedených limitů postupem dle Smlouvy, toto platí i za situace, kdy předmětné Služby nebude možné nadále poskytovat bez překročení předmětných limitů.

6.9. Výše uvedené Ceny za Službu jsou sjednány dohodou Smluvních stran podle zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů, a jsou cenami maximálními a nepřekročitelnými, které zahrnují veškeré náklady spojené s realizací Služeb, zejm. dokumentaci, dopravu do Míst plnění, cestovné, zajištění povinností dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů apod.

6.10. Paušální ceny a Cena za Cloudové služby budou hrazeny zpětně vždy za každý uplynulý kalendářní měsíc poskytování Infra služeb a/nebo Provozních služeb a/nebo Cloudových služeb, a to na základě Objednatelem akceptovaného Záznamu za předmětné období na základě vystavené faktury. Aniž by bylo dotčeno vše uvedené výše v tomto odstavci, Smluvní strany souhlasí s tím, že Cloudové služby pro prostředí TEST a/nebo VÝVOJ budou poskytovány na základě Požadavků k čerpání Cloudových služeb TEST a/nebo VÝVOJ, který vždy přesně definuje dobu zahájení a/nebo dobu ukončení poskytování Cloudové služby pro prostředí TEST a/nebo VÝVOJ. Takto poskytnutá Cloudová služba pro prostředí TEST a/nebo VÝVOJ bude fakturována v rozsahu stanoveném Požadavkem k čerpání Cloudových služeb TEST a/nebo VÝVOJ. Spolu s čerpáním Cloudových služeb v režimu TEST a/nebo VÝVOJ budou vždy čerpány Provozní služby v režimu TEST a/nebo VÝVOJ a dále Infra služby v režimu TEST a/nebo VÝVOJ, které budou fakturovány rovněž v rozsahu stanoveném Požadavkem k čerpání Cloudových služeb TEST a/nebo VÝVOJ.

6.11. Přílohu faktury na Paušální ceny a Cenu za Cloudové služby musí tvořit kopie potvrzeného Záznamu za příslušné období, přičemž dnem uskutečnění zdanitelného plnění je poslední den kalendářního měsíce, v němž byly předmětné Služby poskytnuty.

6.12. Smluvní strany tímto sjednávají výjimku pro účely vyúčtování ZNaCh, kdy Poskytovatel vystaví Objednateli samostatnou fakturu za uplynulý kalendářní měsíc dle skutečné spotřeby na základě odečtu elektroměru, hodnoty PUE a daňového dokladu dodavatele elektrické energie, jehož kopie bude připojena k příslušné faktuře s tím, že DUZP bude datum zjištění. V Záznamu bude uvedena skutečná spotřeba elektrické energie odečtená z elektroměru za daný kalendářní měsíc a platná hodnota PUE.

6.13. Cena za Poskytování odborných rolí dle příslušné Výzvy k poskytování odborných rolí bude hrazena měsíčně, a to na základě Výkazu podepsaného Objednatelem bez výhrad. Kopie Výkazu bude tvořit přílohu faktury. Poskytovatel je oprávněn fakturovat Cenu za Poskytování odborných rolí nejdříve den následující po dni podpisu Výkazu Objednatelem bez výhrad.

6.14. Poskytovatel doručí příslušnou fakturu prostřednictvím datové schránky Objednatele.

6.15. Faktura musí obsahovat náležitosti obchodní listiny dle § 435 OZ a v případě, že jde o daňový doklad, také náležitosti dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Faktura musí dále obsahovat:

6.15.1. přesnou specifikaci Služeb, za které se fakturuje;

6.15.2. specifikaci období, za které se fakturuje;

6.15.3. číslo Smlouvy, popř. číslo Výzvy k poskytování odborných rolí;

6.15.4. Cenu/Ceny za Službu bez DPH a s DPH;

6.15.5. úplné bankovní spojení Poskytovatele, přičemž číslo účtu musí odpovídat číslu účtu uvedenému v záhlaví této Smlouvy nebo číslu účtu v registru plátců DPH, popř. řádně oznámenému číslu účtu postupem dle této Smlouvy.

6.16. Splatnost řádně vystavené faktury činí 30 kalendářních dnů ode dne řádného doručení faktury Objednateli.

6.17. Pokud nebude faktura obsahovat stanovené náležitosti nebo v ní nebudou správně uvedené požadované údaje či bude chybět některá z příloh, je Objednatel oprávněn vrátit ji Poskytovateli ve lhůtě 10 dnů ode dne doručení faktury s uvedením chybějících náležitostí nebo nesprávných údajů, aniž by došlo k prodlení s její úhradou. Ode dne doručení opravené faktury běží Objednateli nová lhůta splatnosti v délce 30 kalendářních dnů.

6.18. Platby dle této Smlouvy budou probíhat výhradně v korunách českých a rovněž veškeré cenové údaje budou uvedeny v této měně.

6.19. V případě uvedení odlišných bankovních údajů na faktuře mají přednost údaje uvedené v záhlaví této Smlouvy nebo číslo účtu v registru plátců DPH, a to až do doby řádného oznámení změny bankovních údajů postupem dle této Smlouvy.

6.20. Aniž by byly dotčeny předcházející odstavce, Poskytovatel bere na vědomí, že Objednatel neposkytuje zálohy na poskytnutí Služeb.

6.21. Poskytovatel prohlašuje, že správce daně před uzavřením Smlouvy nerozhodl o tom, že Poskytovatel je nespolehlivým plátcem ve smyslu § 106a zákona o DPH (dále jen „**Nespolehlivý plátce**"). V případě, že správce daně rozhodne o tom, že Poskytovatel je Nespolehlivým plátcem, zavazuje se Poskytovatel o tomto informovat Objednatele, a to do 2 pracovních dnů od vydání takového rozhodnutí. Stane-li se Poskytovatel Nespolehlivým plátcem, může uhradit Objednatel Poskytovateli pouze základ daně, přičemž DPH bude Objednatelem uhrazena Poskytovateli až po písemném doložení Poskytovatele o jeho úhradě této DPH příslušnému správci daně.

6.22. Poskytovatel je oprávněn zvýšit každou z Cen za Službu dle této Smlouvy s účinností od 1. dubna každého kalendářního roku následujícího po roce 2026 o přírůstek průměrného ročního indexu spotřebitelských cen (dále jen „**Míra inflace**") vyhlášeného Českým statistickým úřadem za předcházející kalendářní rok.

6.23. Poskytovatel je oprávněn zvýšit každou z Cen za Službu podle předcházejícího odstavce pouze v případě, že Míra inflace přesáhne 2 %. Pro vyloučení pochybností se sjednává, že v případě záporné Míry inflace se žádná z Cen za Službu nesnižuje. Poskytovatel je v každém roce oprávněn zvýšit každou Cenu za Službu nejvýše o 10 %; to platí i v případě, že Míra inflace za předcházející kalendářní rok bude vyšší.

6.24. Nebude-li oznámení o zvýšení každé z Cen za Službu doručeno Objednateli do 31. března daného kalendářního roku, právo na uplatnění zvýšení Ceny za Službu v daném kalendářním roce zanikne. Pro vyloučení pochybností Smluvní strany sjednávají, že za účelem zvýšení kterékoliv z Cen za Službu dle odst. 6.21 až odst. 6.23 tohoto článku není nutné uzavírat dodatek ke Smlouvě.

VII. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

7.1. Poskytovatel se zavazuje poskytovat Služby řádně a včas bez faktických a právních vad a v kvalitě definované v jednotlivých SLA dle Přílohy č. 1 Smlouvy.

7.2. Poskytovatel se zavazuje postupovat při realizaci Služeb s odbornou péčí, podle nejlepších znalostí a schopností a sledovat a chránit oprávněné zájmy Objednatele a postupovat v souladu s jeho pokyny a interními předpisy souvisejícími se Službami, které Objednatel Poskytovateli poskytne, nebo s pokyny jím pověřených osob.

7.3. Poskytovatel se zavazuje bez zbytečného odkladu oznámit Objednateli veškeré skutečnosti, které mohou mít vliv na povahu nebo na podmínky poskytování Služeb dle Smlouvy.

7.4. Poskytovatel se zavazuje informovat bezodkladně Objednatele o všech okolnostech důležitých pro řádné a včasné plnění Smlouvy.

7.5. Poskytovatel se zavazuje nakládat se všemi věcmi, dokumenty a dalšími písemnostmi, které mu byly Objednatelem svěřeny za účelem plnění této Smlouvy, s péčí řádného hospodáře a chránit je před poškozením a zneužitím. Objednatel zůstává vlastníkem takových podkladů poskytnutých Poskytovateli za účelem plnění této Smlouvy. Poskytovatel je oprávněn s podklady nakládat pouze v souladu s podmínkami této Smlouvy. Poskytovatel není oprávněn k jinému nakládání a užití podkladů bez předchozího písemného souhlasu Objednatele. Všechny písemnosti a jiné nosiče informací, včetně případných kopií, je povinen chránit před nepovolanými osobami. Poskytovatel plně odpovídá za škodu způsobenou ztrátou a zneužitím hodnot dle tohoto odstavce. Poskytovatel se zavazuje vrátit Objednateli veškeré věci, dokumenty a jiné písemnosti, které mu byly Objednatelem svěřeny pro účely plnění Smlouvy, a to nejpozději do 5 dnů od ukončení Smlouvy, nedohodnou-li se Smluvní strany jinak.

7.6. Poskytovatel se zavazuje nakládat s veškerým SW, včetně případných databází, který Objednatel v rámci součinnosti poskytl či zpřístupnil Poskytovateli výhradně na základě souhlasu Objednatele poskytnutého formou zápisu z jednání Týmu přípravy a poskytování Služby dle Přílohy č. 4 Smlouvy a tak, aby nedošlo k jeho zneužití a využívat jej výhradně za účelem plnění této Smlouvy. V případě porušení této povinnosti odpovídá Poskytovatel za škodu způsobenou Objednateli či třetím osobám.

7.7. Objednatel se zavazuje poskytovat Poskytovateli úplné, pravdivé a včasné informace potřebné k řádnému a včasnému poskytování Služeb.

7.8. Objednatel se zavazuje zaplatit za řádně poskytnuté Služby nebo jejich část cenu dle této Smlouvy.

7.9. Poskytovatel je na vyžádání Objednatele povinen umožnit Objednateli auditovat a provádět analýzu rizik vnitřních procesů Poskytovatele souvisejících s plněním této Smlouvy Poskytovatel je povinen při těchto auditech a analýzách spolupracovat a poskytovat součinnost v míře umožňující provedení řádného auditu a analýzy rizik.

VIII. PODDODAVATELÉ

8.1. Poskytovatel se zavazuje poskytovat plnění dle Smlouvy sám nebo prostřednictvím poddodavatelů. Poskytovatel se zavazuje písemně informovat Objednatele o všech svých poddodavatelích (včetně jejich identifikačních a kontaktních údajů a o tom, kterou část Služby pro něj v rámci plnění Smlouvy každý z poddodavatelů poskytuje) a o jejich změně, a to nejpozději do 10 pracovních dnů ode dne, kdy nastala taková změna nebo kdy Poskytovatel s poddodavatelem vstoupil ve smluvní vztah. Poskytovatel se zavazuje zajistit, že případným využitím poddodavatelů nedojde k porušení ZZVZ, zejména ustanovení § 11 odst. 1.

8.2. Zadání provedení části Služeb poddodavateli Poskytovatelem nezbavuje Poskytovatele jeho výlučné odpovědnosti za řádné provedení Služeb vůči Objednateli. Poskytovatel odpovídá Objednateli za poskytnutí Služeb, které svěří poddodavateli, ve stejném rozsahu, jako by je poskytl sám. Poskytovatel se zavazuje zavázat své poddodavatele k dodržování veškerých relevantních ujednání mezi Objednatelem a Poskytovatelem tak, aby byla v souladu s požadavky Objednatele na Poskytovatele.

IX. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

9.1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace, jakož i jakoukoliv jinou součinnost nezbytnou pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat bezodkladně druhou Smluvní stranu o veškerých skutečnostech, které jsou, nebo mohou být, důležité pro řádné plnění Smlouvy.

9.2. Smluvní strany se zavazují vytvořit pro poskytování součinnosti v rámci svých organizačních struktur optimální komunikační, řídicí a odborné podmínky.

9.3. Smluvní strany jsou povinny dodržovat veškeré platné obecně závazné právní předpisy a závazné normy týkající se předmětu plnění, bezpečnosti a ochrany zdraví při práci, ochrany životního prostředí, likvidace odpadů a norem systému řízení bezpečnosti informací.

9.4. Komunikace mezi Smluvními stranami, související s řízením provozu Služeb, bude probíhat prostřednictvím Oprávněných osob Smluvních stran. Popis činností, jejich odpovědnosti a kompetence jsou uvedeny v Příloze č. 4 Smlouvy.

9.5. Je-li Objednatel v prodlení s poskytnutím součinnosti Poskytovateli a má-li toto prodlení Objednatele za následek nesplnění určité povinnosti Poskytovatele včas, není toto nesplnění povinnosti Poskytovatele včas považováno za prodlení.

X. MLČENLIVOST, OCHRANA A BEZPEČNOST INFORMACÍ

10.1. Obě Smluvní strany se zavazují, že zachovají minimálně jako neveřejné, tj. udrží v tajnosti, podniknou všechny nezbytné kroky k zabezpečení a nezpřístupní třetím osobám informace a zprávy týkající se vlastní spolupráce a vnitřních záležitostí Smluvních stran, pokud by jejich zveřejnění mohlo poškodit druhou Smluvní stranu (dále jen „**Neveřejné informace**“). Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, tím není dotčena. Za Neveřejné informace se považuji veškeré následující informace:

10.1.1. veškeré informace poskytnuté si Smluvními stranami v souvislosti s plněním této Smlouvy (pokud nejsou výslovně obsaženy ve znění Smlouvy zveřejňovaném dle čl. XVII odst. 17.6 Smlouvy);

10.1.2. informace, na které se vztahuje zákonem uložená povinnost mlčenlivosti;

10.1.3. veškeré další informace, které budou Smluvními stranami označeny minimálně jako neveřejné.

10.2. Povinnost zachovávat mlčenlivost uvedená v odst. 10.1 tohoto článku se nevztahuje na informace:

10.2.1. které jsou Smluvní strany povinny poskytnout třetím osobám podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů;

10.2.2. jejichž sdělení vyžaduje jiný právní předpis;

10.2.3. které jsou nebo se stanou všeobecně a veřejně přístupnými jinak než porušením právních povinností ze strany některé ze Smluvních stran;

10.2.4. u nichž jsou Smluvní strany schopny prokázat, že jim byly známy ještě před přijetím těchto informací od druhé Smluvní strany, avšak pouze za podmínky, že se na tyto informace nevztahuje povinnost mlčenlivosti z jiných důvodů;

10.2.5. které budou Smluvní straně po uzavření této Smlouvy sděleny bez závazku mlčenlivosti třetí stranou, jež rovněž není ve vztahu k těmto informacím nijak vázána.

10.3. Jako s Neveřejnými informacemi musí být nakládáno také s informacemi, které splňují podmínky uvedené v odst. 10.1. tohoto článku, i když byly získány náhodně nebo bez vědomí druhé Smluvní strany a dále s veškerými informacemi získanými od jakékoliv třetí strany, pokud se týkají Smluvní strany nebo plnění této Smlouvy.

10.4. Smluvní strany se zavazují, že Neveřejné informace užijí pouze za účelem plnění této Smlouvy. K jinému užití je zapotřebí písemného souhlasu druhé Smluvní strany.

10.5. Poskytovatel je povinen svého případného poddodavatele zavázat povinností mlčenlivosti a respektováním práv Objednatele nejméně ve stejném rozsahu, v jakém je zavázán sám touto Smlouvou.

10.6. Povinnost mlčenlivosti dle této Smlouvy trvá i po naplnění této Smlouvy bez ohledu na zánik ostatních závazků ze Smlouvy, a to v případě Neveřejných informací po dobu 5 let ode dne ukončení Smlouvy, pokud nebude povinnosti mlčenlivosti dříve daná Smluvní strana druhou Smluvní stranou písemně zproštěna.

10.7. Závazky vyplývající z tohoto článku není žádná ze Smluvních stran oprávněna vypovědět ani jiným způsobem jednostranně ukončit.

10.8. Smluvní strany berou na vědomí, že vzhledem k tomu, že s plněním této Smlouvy je spojeno zpracování osobních údajů pracovníků Objednatele a případně rovněž dodavatelů Objednatele – podnikajících fyzických osob, které poskytují Objednateli v rámci pracovněprávních a obchodních vztahů (dále jen „**Osobní údaje**“) ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „**Obecné nařízení**“), je pro účely této Smlouvy Objednatel v postavení správce Osobních údajů (pro účely tohoto odstavce dále jen „**Správce**“) a Poskytovatel v postavení zpracovatele Osobních údajů (pro účely tohoto odstavce dále jen „**Zpracovatel**“), přičemž Zpracovatel a Správce se zavazují za účelem plnění Smlouvy uzavřít písemnou smlouvu o zpracování osobních údajů reflektující povinnosti dle Obecného nařízení, zákona č. 110/2019 Sb., o zpracování osobních údajů jakožto prováděcího předpisu k Obecnému nařízení a příslušných právních předpisů.

XI. KYBERNETICKÁ BEZPEČNOST

11.1. Poskytovatel se zavazuje při plnění této Smlouvy postupovat v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění (dále též „**ZoKB**“), jakož i v souladu se souvisejícími prováděcími předpisy a vnitřními předpisy Objednatele, jejichž předání proběhne na základě oboustranně podepsaného předávacího protokolu, který obsahuje seznam předávané dokumentace.

11.2. Poskytovatel bere na vědomí, že předmět plnění dle této Smlouvy souvisí s podporou provozu, užitím, správou, či rozvojem Kritické informační infrastruktury ve smyslu ustanovení § 2 písm. b) ZoKB, Významných informačních systémů ve smyslu ustanovení § 2 písm. d) ZoKB, a ostatních informačních systémů Objednatele provozovaných v infrastruktuře Poskytovatele. Klasifikace jednotlivých systémů dle ZoKB je uvedena k příloze č. 1.

11.3. Poskytovatel bere na vědomí, že v souvislosti se Službami dle této Smlouvy se stává Významným dodavatelem ve smyslu ustanovení § 2 písm. n) VoKB a provozovatelem ve smyslu ustanovení § 2 písm. g) ZoKB.

11.4. Poskytovatel se zavazuje v průběhu plnění této Smlouvy písemně upozornit Objednatele na případný zjištěný nesoulad plnění dle odst. 11.1 a 11.3 tohoto článku této Smlouvy s povinnostmi definovanými ZoKB a s případnými nedostatky zjištěnými auditem kybernetické bezpečnosti.

11.5. V případě kybernetického bezpečnostního incidentu (dále též „**KBI**") vzniklého při poskytování Služeb dle této Smlouvy, se Poskytovatel zavazuje tento KBI neprodleně oznámit Objednateli a následně přijmout opatření pro odvrácení a zmírnění dopadu KBI, a to vše na vlastní náklady. Poskytovatel informuje Objednatele o odstranění nahlášeného KBI a po uzavření KBI sepíše akceptační protokol (viz Příloha č. 6 této Smlouvy - Vyhodnocení / akceptační protokol o odstranění kybernetické bezpečnostní události - incidentu) o odstranění KBI, který bude obsahovat mimo jiné popis závady, případně důvod jejího vzniku, způsob odstranění závady, a po tom, co Objednatel akceptuje, že je závada kompletně odstraněna, podpisy Poskytovatele a Objednatele, přičemž Objednatele bude ve věcech kybernetické bezpečnosti zastupovat Manažer kybernetické bezpečnosti Ministerstva financí. Poskytovatel se zavazuje umožnit Objednateli provést kontrolu procesu odstraňování KBI a vypořádat se s případnými připomínkami Objednatele k procesu odstraňování KBI.

11.6. Kontrola zavedení a užití bezpečnostních opatření a procesů:

11.6.1. Poskytovatel se na výzvu zavazuje umožnit Objednateli provedení kontroly v rozsahu zavedení a realizace bezpečnostních opatření, jejichž zavedení a užití je vyžadováno ZoKB, prováděcími předpisy k tomuto zákonu nebo vnitřními předpisy Objednatele předanými podle odst. 11.1 tohoto článku. Výzva na Poskytovatele bude zaslána minimálně 1 měsíc před takovou kontrolou a součástí výzvy bude rozsah kontrolovaných oblastí a bezpečnostních opatření. Poskytovatel vyhotoví písemné stanovisko k Výzvě do 5 pracovních dnů od doručení Výzvy a v případě nesouhlasu s požadavky Výzvy předloží současně toto stanovisko k projednání ŘKO dle Přílohy č. 4 této Smlouvy. Poskytovatel poskytne Objednateli, nebo jím určené třetí straně, nutnou součinnost při provedení kontroly. Z kontroly vyhotoví Objednavatel dokument s názvem „Zápis z kontroly Zhotovitele/Poskytovatele služby" (dále též „**Zápis**").

11.6.2. Při každé kontrole bude vždy přihlédnuto k rozsahu plnění dle rozsahu pověření podle ustanovení § 8 Řízení dodavatelů, odst. 1 písm. a) VoKB.

11.6.3. Pokud bude během kontroly zjištěno, že Poskytovatel v některé předepsané oblasti nesplňuje povinné náležitosti, tj. bezpečnostní, organizační a technická opatření nejsou zavedena nebo užita, nebo jsou zavedena či užita v nedostatečném rozsahu, je tato skutečnost zapsána do Zápisu, včetně navržení lhůty pro Poskytovatele k odstranění zjištěných nedostatků při kontrole. Poskytovatel vyhotoví písemné stanovisko k tomuto Zápisu do 10 pracovních dnů od doručení Zápisu a ve stejné lhůtě předloží toto stanovisko k projednání ŘKO dle Přílohy č. 4 této Smlouvy. ŘKO následně určí závaznou lhůtu pro Poskytovatele k odstranění zjištěných nedostatků a současně rozsah potřebné součinnosti ze strany Objednatele.

11.7. Poskytovatel akceptuje, že veškeré náklady, které mu v průběhu plnění dle této Smlouvy vzniknou v souvislosti s výše uvedenými kontrolami, se zavedením a plněním požadavků dle ZoKB, s provedeným auditem kybernetické bezpečnosti či užitím definovaných bezpečnostních opatření, jsou plně k jeho tíži.

11.8. Seznam vyžadovaných bezpečnostních opatření se může měnit v návaznosti na povinnosti Objednatele vyplývající z § 11 ZoKB. Pokud Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) Objednateli uloží povinnost zavést či užívat určité bezpečnostní opatření, dotýká – li se toto jakkoliv povahy či rozsahu plnění dle této Smlouvy, má Poskytovatel povinnost toto bezpečnostní opatření zavést či užívat, nebo Objednateli poskytnout nutnou součinnost k zajištění uložených povinností.

XII. VLASTNICKÉ PRÁVO, NEBEZPEČÍ ŠKODY A PRÁVA TŘETÍCH OSOB

12.1. Poskytovatel prohlašuje, že vlastnické právo a nebezpečí škody na věci ke všem hmotným výstupům, tj. technickým nosičům dokumentů (např. CD, flashdisk apod.) či dokumentům v listinné podobě vytvořeným a předaným Poskytovatelem Objednateli v souvislosti s poskytováním Služeb v rámci Smlouvy přechází na Objednatele dnem jejich protokolárního předání Objednateli.

12.2. Poskytovatel prohlašuje, že Služby a jejich případné výstupy budou bez právních vad, zejména, že nebudou zatíženy žádnými právy třetích osob, z nichž by pro Objednatele vyplynul finanční nebo jiný závazek ve prospěch třetí strany nebo která by jakkoliv omezovala užívání výstupů Služeb.

12.3. Poskytovatel se zavazuje, že při plnění Smlouvy bude postupovat tak, aby nedošlo k neoprávněnému zásahu do práv třetích osob.

12.4. Udělení veškerých práv uvedených v tomto článku Smlouvy nelze ze strany Poskytovatele vypovědět a na jejich udělení nemá vliv ukončení účinnosti Smlouvy, pokud nastalo po okamžiku rozhodném pro udělení předmětného práva.

12.5. Dojde-li při poskytování Služeb dle této Smlouvy k vytvoření či poskytnutí autorského díla či databáze dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů poskytuje Poskytovatel Objednateli k takovému autorskému dílu, resp. databázi, výhradní oprávnění ke všem způsobům užití (včetně zdrojových kódů ve spustitelné formě) zejména k jeho rozmnožování, rozšiřování, pronájmu, půjčování, vystavování, sdělování veřejnosti, resp. databázi vytěžovat a zužitkovat, dle účelu této Smlouvy, a to v územně a množstevně neomezeném rozsahu, po celou dobu trvání autorských práv autora a dále též právo postoupení nebo poskytnutí oprávnění tvořící součást této licence (podlicenci) jakékoliv třetí osobě, a to včetně svolení autorské dílo a/nebo databázi měnit, spojovat s jinými díly a zařazovat je do děl souborných.

XIII. SANKČNÍ UJEDNÁNÍ

13.1. Smluvní pokuta za nesplnění kvalitativních parametrů poskytování příslušné Služby, příp. Služeb Poskytovatelem je uvedena v Příloze č. 1 Smlouvy.

13.2. V případě, že Poskytovatel poruší některou z povinností dle čl. VIII (Poddodavatelé) a/nebo dle čl. XI odst. 11.4 a/nebo 11.5 této Smlouvy (Kybernetická bezpečnost) je Objednatel oprávněn požadovat smluvní pokutu ve výši 50 000 Kč, a to každý jednotlivý případ porušení.

13.3. V případě, že Poskytovatel poruší povinnost udržovat v platnosti a účinnosti po celou dobu účinnosti Smlouvy pojistnou smlouvu dle čl. XIV odst. 14.6 Smlouvy vzniká Objednateli nárok na smluvní pokutu ve výši 100 000 Kč za každý i započatý měsíc, v němž nebude mít účinnou pojistnou smlouvu se stanovenými parametry.

13.4. V případě, že Poskytovatel bude v prodlení se lhůtou dle čl. XI odst. 11.6 pododst. 11.6.3 Smlouvy pro odstranění zjištěných nedostatků v bezpečnostních, organizačních a technických opatřeních KB stanovenou a schválenou ze strany ŘKO, vzniká Objednateli nárok na smluvní pokutu ve výši 50 000 Kč, a to za každý i započatý den prodlení.

13.5. V případě, že některá ze Smluvních stran poruší některou z povinností dle čl. X (Mlčenlivost) a/nebo čl. XVII odst. 17.10 této Smlouvy (zákaz postoupení závazku ze Smlouvy), je druhá Smluvní strana oprávněna požadovat smluvní pokutu ve výši 100 000 Kč, a to za každý jednotlivý případ porušení.

13.6. Smluvní pokuta a zákonný úrok z prodlení jsou splatné ve lhůtě 30 dnů ode dne doručení písemné výzvy formou vystavené faktury na sankci oprávněné Smluvní strany Smluvní straně povinné ze smluvní pokuty nebo ze zákonného úroku z prodlení.

13.7. Pro případ prodlení Objednatele se zaplacením řádně vystavené a doručené faktury je Poskytovatel oprávněn požadovat zaplacení úroku z prodlení ve výši stanovené právními předpisy.

13.8. Odstoupení od Smlouvy ze strany Objednatele či Poskytovatele nesmí být spojeno s uložením jakékoliv sankce k tíži Objednatele či Poskytovatele.

13.9. Ujednáním o smluvní pokutě není dotčeno právo poškozené Smluvní strany domáhat se náhrady škody v souladu s čl. XIV Smlouvy.

13.10. Aniž by byl dotčen předcházející odstavec, Smluvní strany se výslovně dohodly, že celková výše všech nároků na smluvní pokuty vzniklých na základě nebo v souvislosti s touto Smlouvou jedné Smluvní straně se omezuje částkou odpovídající 200 000 000 Kč.

13.11. Zaplacení smluvní pokuty nezbavuje Smluvní stranu povinnosti splnit závazek utvrzený smluvní pokutou.

13.12. Po dobu zásahu vyšší moci a po dobu nezbytnou k odstranění těchto zásahů nebo vlivem skutečností, při nichž nelze spravedlivě po Poskytovateli požadovat plnění provedené řádně a včas, Poskytovatel není v prodlení s plněním své smluvní povinnosti. Termín plnění se posunuje o dobu tomuto odpovídající. O takové skutečnosti je Poskytovatel povinen v přiměřené době Objednatele informovat a sdělit mu předpokládaný náhradní termín plnění. Za vyšší moc se považuje mimořádná nepředvídatelná a neodvratitelná událost, která nastala nezávisle na vůli Poskytovatele, které nelze zabránit ani při vynaložení veškerého možného úsilí, zejména např. přírodní katastrofa, živelná pohroma, teroristický útok, válka, stávka, povstání či vojenská akce.

XIV. NÁHRADA ÚJMY

14.1. Smluvní strany sjednávají, že náhrada újmy se bude řídit právními předpisy, není-li ve Smlouvě sjednáno jinak.

14.2. Smluvní strany odpovídají za každé zaviněné porušení smluvní povinnosti.

14.3. Smluvní strany se dohodly, že omezují právo na náhradu újmy, která může při plnění Smlouvy jedné Smluvní straně vzniknout, a to na celkovou částku odpovídající částce 200 000 000 Kč. Ustanovení § 2898 OZ není tímto ujednáním dotčeno, tj. uvedené omezení náhrady újmy se neuplatní u újmy způsobené člověku na jeho přirozených právech, anebo způsobené úmyslně či hrubou nedbalostí.

14.4. Újmu hradí škůdce v penězích, nepožaduje-li poškozený uvedení do předešlého stavu.

14.5. Náhrada újmy je splatná ve lhůtě 30 dnů od doručení písemné výzvy oprávněné Smluvní strany Smluvní straně povinné z náhrady újmy.

14.6. Poskytovatel se zavazuje mít po celou dobu účinnosti Smlouvy sjednanou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu (újmu) způsobenou jeho činností v souvislosti s poskytováním Služeb Objednateli, případně třetím osobám, a to ve výši pojistného plnění minimálně 200 000 000 Kč. Na požádání je Poskytovatel povinen Objednateli takovou aktuálně platnou pojistnou smlouvu nebo pojistný certifikát osvědčující uzavření takové pojistné smlouvy do 3 pracovních dnů předložit.

XV. ODPOVĚDNOST ZA VADY

15.1. Poskytovatel se zavazuje, že Službu poskytne v souladu se Smlouvou, a že po dobu účinnosti Smlouvy bude mít dohodnuté vlastnosti, úroveň a charakteristiky. Objednatel je povinen za řádně poskytnutou Službu uhradit Poskytovateli cenu dle čl. VI Smlouvy. Při nedodržení těchto povinností se jedná o vadné plnění dle této Smlouvy.

15.2. Pro vyloučení pochybností Smluvní strany uvádějí, že Poskytovatel není v rámci odpovědnosti za vady odpovědný za:

15.2.1. poruchy vyvolané připojením a použitím jakéhokoliv zařízení či SW, které není oběma Smluvními stranami schválenou součástí komunikačního rozhraní systému, infrastruktury Objednatele či schválenou součástí implementovaného systému;

15.2.2. poruchy vyvolané instalací či reinstalací HW a SW, komunikační a aplikační infrastruktury, či změny jejich konfigurací provedené Objednatelem bez předchozí písemné dohody s Poskytovatelem;

15.2.3. skutečnost, kdy Objednatel neumožní přístup Poskytovateli k HW a SW pro výkon poskytování Služby, resp. servisních činností;

15.2.4. zásah nezaškolené obsluhy či třetí osoby odlišné od Poskytovatele nebo jeho poddodavatele. Za zaškolení obsluhy je zodpovědná každá ze Smluvních stran na zařízeních, která provozuje. Zaškolená osoba získá certifikát, kterým se lze prokázat.

15.3. Poskytovatel je povinen poskytovat Služby v dohodnuté kvalitě a odpovídá za to, že případné vady Služeb řádně odstraní, přičemž se zavazuje vady odstranit v rámci poskytované Služby v souladu s Přílohou č. 1 Smlouvy.

15.4. Ustanovením tohoto článku Smlouvy nejsou dotčena ani omezena práva Objednatele z vadného plnění vyplývající z právních předpisů.

XVI. DOBA TRVÁNÍ SMLOUVY A UKONČENÍ SMLOUVY

16.1. Tato Smlouva se uzavírá na dobu určitou, tj. do 31. 03. 2028 s účinností ode dne zveřejnění Smlouvy v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv v platném znění (dále jen „**ZRS**“) nebo od 1. 4. 2024, podle toho, která ze skutečností nastane později. Dle dohody Smluvních stran tuto Smlouvu v registru smluv uveřejní Objednatel a o jejím uveřejnění bude prostřednictvím e-mailové zprávy informovat Oprávněnou osobu Poskytovatele.

16.2. Smlouvu lze ukončit písemnou dohodou Smluvních stran podepsanou osobami oprávněnými jednat za Smluvní strany, přičemž účinky ukončení Smlouvy nastanou k okamžiku stanovenému v takové dohodě. Nebude-li takový okamžik stanoven, pak tyto účinky nastanou ke dni účinnosti dohody, tj. ke dni zveřejnění v registru smluv.

16.3. Každá ze Smluvních stran je oprávněna Smlouvu vypovědět, a to i bez udání důvodu. Výpovědní doba Smlouvy činí 12 měsíců a počíná běžet prvním dnem měsíce následujícího po měsíci, ve kterém bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé Smluvní straně.

16.4. Smlouva může zaniknout odstoupením příslušné Smluvní strany, nastanou-li okolnosti předvídané § 2002 OZ.

16.5. Odstoupením se závazek založený touto Smlouvou zrušuje pouze ohledně nesplněného zbytku plnění (tj. ex nunc). Smluvní strany si jsou povinny vyrovnat dosavadní vzájemné závazky ze Smlouvy, a to bez zbytečného odkladu, nejpozději však do 30 dnů od doručení oznámení Smluvní strany o odstoupení od Smlouvy druhé Smluvní straně.

16.6. Za podstatné porušení Smlouvy Poskytovatelem se považuje zejména prodlení Poskytovatele s plněním jakýchkoliv lhůt ze Smlouvy o více než 30 kalendářních dnů.

16.7. Za podstatné porušení Smlouvy Objednatelem ve smyslu § 2002 OZ se považuje zejména prodlení Objednatele s úhradou faktury o více než 30 kalendářních dnů.

16.8. Objednatel je dále oprávněn od Smlouvy odstoupit v případě, že:

16.8.1. bude rozhodnuto o likvidaci Poskytovatele;

16.8.2. Poskytovatel podá insolvenční návrh ohledně své osoby, bude rozhodnuto o úpadku Poskytovatele nebo bude ve vztahu ke Poskytovateli vydáno jiné rozhodnutí s obdobnými účinky;

16.8.3. Poskytovatel bude pravomocně odsouzen za úmyslný majetkový nebo hospodářský trestný čin;

16.8.4. Poskytovatel se stane Nespolehlivým plátcem;

16.8.5. dojde k významné změně kontroly nad Poskytovatelem nebo změny kontroly nad zásadními aktivy, využívanými Poskytovatelem k plnění této Smlouvy, přičemž kontrolou se zde rozumí vliv, ovládání či řízení dle ust. § 71 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) (dále jen „**ZOK**"), či ekvivalentní postavení.

16.9. Nastane-li některý z případů uvedených v odst. 16.8. pododst. 16.8.1. až 16.8.5. tohoto článku Smlouvy, je Poskytovatel povinen informovat o této skutečnosti Objednatele písemně do 2 (dvou) dnů od jejího vzniku, společně s informací o tom, o kterou skutečnost jde, s uvedením bližších údajů, které by Objednatel mohl v této souvislosti potřebovat pro své rozhodnutí o odstoupení od Smlouvy. Nedodržení této povinnosti je podstatným porušením Smlouvy.

16.10. Odstoupení od Smlouvy musí být písemné, jinak nemá právní účinky. Odstoupení je účinné ode dne, kdy bylo doručeno druhé Smluvní straně. V pochybnostech se má za to, že odstoupení od Smlouvy bylo doručeno pátým kalendářním dnem od jeho odeslání příslušné Smluvní straně doporučenou poštovní zásilkou nebo jeho doručením do datové schránky příslušné Smluvní straně při odeslání datovou zprávou.

16.11. Ukončením Smlouvy nejsou dotčena práva na zaplacení smluvní pokuty nebo zákonného úroku z prodlení, pokud už dospěl, práva na náhradu újmy, povinnosti mlčenlivosti dle čl. X Smlouvy, práva z odpovědnosti za vady a záruky ani další ujednání, z jejichž povahy vyplývá, že mají zavazovat Smluvní strany i po zániku účinnosti této Smlouvy.

XVII. ZÁVĚREČNÁ USTANOVENÍ

17.1. Jakékoliv úkony směřující k ukončení této Smlouvy a oznámení o změně bankovních údajů musí být doručeny datovou schránkou nebo formou doporučeného dopisu. Oznámení nebo jiná sdělení podle této Smlouvy se budou považovat za řádně učiněná, pokud budou učiněna písemně v českém jazyce a doručena, osobně, poštou či prostřednictvím datové schránky na adresy uvedené v tomto článku (včetně označení jménem příslušné Oprávněné osoby) nebo na jinou adresu, kterou příslušná Smluvní strana v předstihu písemně oznámí adresátovi, není-li v konkrétním případě ve Smlouvě stanoveno jinak:

17.1.1. Objednatel:

Název: Česká republika – Ministerstvo financí
K rukám: jméno Oprávněné osoby Objednatele
Datová schránka: xzeaauv

17.1.2. Poskytovatel:
Název: Státní pokladna Centrum sdílených služeb, s. p.
K rukám: jméno Oprávněné osoby Poskytovatele
Datová schránka: ag5uunk

17.2. Účinnost oznámení nastává v pracovní den následující po dni doručení tohoto oznámení druhé Smluvní straně, není-li ve Smlouvě v konkrétním případě stanoveno jinak.

17.3. Smluvní strany se dohodly na určení Oprávněné osoby za každou Smluvní stranu (dále jen „**Oprávněná osoba**"). Oprávněné osoby jsou oprávněné ke všem jednáním týkajícím se této Smlouvy, s výjimkou změn nebo zrušení Smlouvy a oznámení o změně bankovních údajů, není-li ve Smlouvě stanoveno jinak. V případě, že Smluvní strana má více Oprávněných osob, zasílají se veškeré e-mailové zprávy na adresy všech Oprávněných osob v kopii:

17.3.1. Oprávněnou osobou Objednatele je:

Jméno: xxx
E-mail: xxx
Telefon: xxx

Jméno: xxx
E-mail: xxx
Telefon: xxx

17.3.2. Oprávněnou osobou Poskytovatele je:
Jméno: xxx
E-mail: xxx
Telefon: xxx

Jméno: xxx
E-mail: xxx
Telefon: xxx

Jméno: xxx
E-mail: xxx
Telefon: xxx

17.4. Ke změně nebo ukončení Smlouvy a k oznámení o změně bankovních údajů je za Objednatele oprávněn xxx, ministr financí a dále osoby pověřené ministrem financí. Ke změně nebo ukončení Smlouvy a k oznámení o změně bankovních údajů je za Poskytovatele oprávněn xxx, generální ředitel a dále osoby pověřené generálním ředitelem. Jiné osoby mohou tato právní jednání činit pouze s písemným pověřením osoby či orgánu vymezených v předchozích větách (dále jen „**Odpovědné osoby pro věci smluvní**"). Odpovědné osoby pro věci smluvní mají současně všechna oprávnění Oprávněných osob.

17.5. Jakékoliv změny kontaktních údajů, bankovních údajů a Oprávněných osob je příslušná Smluvní strana oprávněna provádět jednostranně a je povinna tyto změny neprodleně písemně oznámit druhé Smluvní straně.

17.6. Obě Smluvní strany souhlasí s tím, že podepsaná Smlouva (včetně příloh), jakož i její text, může být zveřejněna v souladu s povinnostmi vyplývajícími z právních předpisů, a to bez časového omezení. Objednatel se zavazuje, že Smlouvu v souladu se Zákonem o registru smluv uveřejní v registru smluv.

17.7. Tato Smlouva se řídí OZ a dalšími příslušnými právními předpisy České republiky.

17.8. Stane-li se kterékoliv ustanovení této Smlouvy neplatným, neúčinným nebo nevykonatelným, zůstává platnost, účinnost a vykonatelnost ostatních ustanovení této Smlouvy nedotčena, nevyplývá-li z povahy daného ustanovení, obsahu Smlouvy, nebo okolnosti, za nichž bylo toto ustanovení vytvořeno, že toto ustanovení nelze oddělit od ostatního obsahu Smlouvy. Smluvní strany se zavazují nahradit po vzájemné dohodě dotčené ustanovení jiným ustanovením, blížícím se svým obsahem nejvíce účelu neplatného či neúčinného ustanovení.

17.9. Jestliže kterákoli ze Smluvních stran neuplatní nárok nebo nevykoná právo podle této Smlouvy, nebo je vykoná se zpožděním nebo pouze částečně, nebude to znamenat vzdání se těchto nároků nebo práv. Vzdání se práva z titulu porušení této Smlouvy nebo práva na nápravu anebo jakéhokoliv jiného práva podle této Smlouvy, musí být vyhotoveno písemně a podepsáno Smluvní stranou, která takové vzdání činí.

17.10. Smluvní strana není oprávněna bez písemného souhlasu druhé Smluvní strany postoupit Smlouvu, jednotlivý závazek ze Smlouvy ani pohledávky vzniklé v souvislosti s touto Smlouvou na třetí osoby, ani učinit jakékoliv právní jednání, v jehož důsledku by došlo k převodu nebo přechodu práv či povinností vyplývajících z této Smlouvy.

17.11. Změny nebo doplňky této Smlouvy včetně příloh musejí být vyhotoveny písemně formou dodatku, datovány a podepsány oběma Smluvními stranami s podpisy Smluvních stran na jedné písemnosti, ledaže Smlouva v konkrétním případě stanoví jinak.

17.12. Smluvní strany se se dohodly, že veškeré spory vyplývající z této Smlouvy nebo spory o existenci této Smlouvy (včetně otázky vzniku a platnosti Smlouvy) budou řešit především dohodou. Nedojde-li k dohodě ani do 60 dnů ode dne zahájení jednání o dohodě, bude předmětný spor rozhodován s konečnou platností před věcně a místně příslušným soudem České republiky, přičemž rozhodným právem, je právo české.

17.13. Smluvní strany se dohodly, že vylučují aplikaci § 557 a § 558 odst. 2 OZ.

17.14. Poskytovatel výslovně prohlašuje, že se podrobně seznámil se všemi dokumenty týkajícími se Služeb, a že žádné z ustanovení tam uvedených nepovažuje za takové, které by nemohl rozumně předpokládat.

17.15. Tato Smlouva je vyhotovena elektronicky v 1 (jednom) vyhotovení v českém jazyce s platností originálu s elektronickými podpisy obou Smluvních stran v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

17.16. Tato Smlouva nabývá platnosti dnem podpisu oběma Smluvními stranami a účinnosti dnem uvedeným v čl. XVI odst. 16.1 Smlouvy.

17.17. Smluvní strany po řádném přečtení této Smlouvy prohlašují, že Smlouva byla uzavřena po vzájemném projednání, na základě jejich pravé, vážně míněné a svobodné vůle, při respektování principu poctivosti, spravedlnosti a rovnosti smluvních stran. Na důkaz uvedených skutečností připojují své podpisy.

17.18. Nedílnou součást Smlouvy tvoří tyto přílohy:

Příloha č. 1: Technická specifikace Služeb
Příloha č. 2: Katalog rolí a ceník rolí
Příloha č. 3: Specifické služby KB

Příloha č. 4: Řízení provozu Služeb
Příloha č. 5: Vzory protokolů a dalších dokumentů
Příloha č. 6: Vyhodnocení / akceptační protokol o odstranění kybernetické bezpečnostní události - incidentu

Za Objednatele:

V Praze dne dle elektronického podpisu

Česká republika – Ministerstvo financí
xxx
xxx

Za Poskytovatele:

V Praze dne dle elektronického podpisu

Státní pokladna Centrum sdílených služeb, s. p
xxx
xxx

Za finální znění k č.j. MF-32883/2023/7001:xxx

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/01	Zajištění a provoz produkčního prostředí IISSP

1 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba 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).

Prostředí testování třetích stran a školení bude poskytováno pouze v režimu 8x5 hodin ve zkrácené provozní době, tj. v pracovních dnech od 8:00 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:

Prostředí pro provoz IISSP – Platforma Power			
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).		
Pre-produktivní			
Testovací			
Vývojové			
Testování třetích stran a školení			
Celkový rezervovaný výkon	**184,5**	**4 021**	**186 402**
Prostředí pro provoz IISSP – 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).		
Pre-produktivní			
Testovací			
Vývojové			
Testování třetích stran a školení			
Celkový rezervovaný výkon	**6**	**28**	**381**

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/ 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 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/01)**		
	bez DPH	**DPH**	**s DPH**
Měsíční cena v období od účinnosti Smlouvy do 31. 03. 2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	5 297 506,00	1 112 476,26	6 409 982,26
2.2 Poskytování správy, servisní podpory SW a údržby HW (Provozní služba)	1 074 938,00	225 736,98	1 300 674,98
2.3 Zajišťování provozu bezpečného komunikačního rozhraní (Provozní služba)	1 975 580,00	414 871,80	2 390 451,80
2.4 Řízení provozu a dohled nad kvalitou poskytovaných služeb (Provozní služba)	439 097,00	92 210,37	531 307,37
Celková měsíční cena	**8 787 121,00**	**1 845 295,41**	**10 632 416,41**

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).

Prostředí pro provoz informačních portálů – MONITOR – Platforma x64			
Prostředí	**CPU**	**RAM (GB)**	
Produktivní	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).		
Pre-produktivní			
Testovací			
Celkový rezervovaný výkon	**4 000 kreditů**		

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) využívá virtuální 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 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 %	95 %
Testovací	95 %	95 %

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 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/02)		
	bez DPH	DPH	s DPH
Měsíční cena v období od účinnosti Smlouvy 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)	1 439,00	302,19	1 741,19
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	**232 668,00**	**48 860,28**	**281 528,28**

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).

Prostředí pro Službu provoz informačních portálů – Platforma x64			
Prostředí	**CPU**	**RAM (GB)**	
Produktivní	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.		
Testovací			
Celkový rezervovaný výkon	**4 000 kreditů**		

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.

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 MF/02 - Hosting aplikace Monitor a 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 účinnosti Smlouvy 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)	101 992,00	21 418,32	123 410,32
Celková měsíční cena	**232 990,00**	**48 927,90**	**281 917,90**

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 24,598 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 účinnosti Smlouvy 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**	**20 500**

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 účinnosti Smlouvy do 31. 03. 2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	68 712,00	14 429,52	83 141,52
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	**478 693,00**	**100 525,53**	**579 218,53**

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>26 071</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	**56**	**1 090**	**798 758**

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	**80**	**280**

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 – 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	<1 500 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 (24x7 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 účinnosti Smlouvy do 31. 03. 2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	186 930,00	39 255,30	226 185,30
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	**1 245 342,00**	**261 521,82**	**1 506 863,82**

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 účinnosti Smlouvy do 31. 03. 2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	2 151 789,00	451 875,69	2 603 664,69
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	**3 123 974,00**	**656 034,54**	**3 780 008,54**

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 účinnosti Smlouvy do 31. 03. 2028			
2.1 Poskytování výpočetního výkonu a zálohovacích kapacit (Infra služba)	333 778,00	70 093,38	403 871,38
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	**593 397,00**	**124 613,37**	**718 010,37**

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		

Testovací	diskový prostor, resp. jejich změny, budou řízení provozu (viz Příloha č. 4 Smlouvy). Výkaz alokace výpočetního výkonu bude Poskytovatel předkládat Objednateli na vyžádání.		
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 účinnosti Smlouvy 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
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 vždy 6 měsíců v období 12 měsíců poskytování služby dle požadavku Objednatele.
Testovací	Prvních 12 měsíců poskytování služby, v následujícím období vždy 6 měsíců v období 12 měsíců poskytování služby 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**

Prostředí pro provoz IS ARES – Platforma MS AZURE		
Prostředí	**vCPU LIN**	**RAM (GB)**
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 – Infra služby

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 účinnosti Smlouvy 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 účinnosti Smlouvy 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

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 účinnosti Smlouvy do 31. 03. 2028			
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
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 účinnosti Smlouvy 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 24,598 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, filesystemy, 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, 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 OpenData který poskytuje podporu Službě MF/02 – Webové portály, 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/02.

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 účinnosti Smlouvy 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 ROČNÍ 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 účinnosti Smlouvy 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 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 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.

SPCSS
Státní pokladna
Centrum sdílených služeb

Příloha č. 2 Katalog rolí a ceník rolí

Role	Popis role
Analytik kybernetické bezpečnosti	Analytik kybernetické bezpečnosti je osoba, která: • provádí hloubkové analýzy kybernetických bezpečnostních udá lostí a incidentů (KBU a KBI); • provádí odborné konzultace (po technické stránce) v oblasti ky bernetické bezpečnosti; • spolupracuje při vyšetřování kybernetických bezpečnostních událostí a incidentů; • komunikuje s odbornou veřejností při výměně zkušeností a sdí lení informací týkajících se kybernetických útoků a způsobech zabezpečení; • zpracovává dokumentaci ve svěřené oblasti kybernetické bez pečnosti; • spolupracuje na analýze, sběru, dekompozici a syntéze získa ných informací a na návrhu implementace bezpečnostního mo nitoringu; • účastní se jednání s pracovníky Objednatele; • zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem; • provádí penetrační testy.
Architekt kybernetické bezpečnosti	Architekt kybernetické bezpečnosti je osoba, která: • zajišťuje povinnosti bezpečnostní role vycházející ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvise-jících zákonů (zákon o kybernetické bezpečnosti); • poskytuje odborné konzultace v oblasti systému řízení bezpeč-nosti informací/kybernetické bezpečnosti; • provádí analýzu, sběr, dekompozici a syntézu získaných infor-mací a navrhuje implementaci bezpečnostního monitoringu; • zajišťuje prosazování bezpečnosti informací v rámci koncepč-ního rozvoje komunikačních a informačních systémů; • účastní se jednání s pracovníky Objednatele; • zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem; na základě analýzy provádí návrhy a předkládá objednateli, následně zajišťuje implementaci vhodných bezpečnostních opatření včetně zajištění příslušné dokumentace.
Manažer rozvoje služeb kybernetické bezpečnosti	Manažer služeb kybernetické bezpečnosti je osoba, která: • poskytuje konzultace v oblasti systému řízení bezpečnosti informací/kybernetické bezpečnosti; • připravuje a prezentuje návrhy možného rozvoje činností v oblasti kybernetické bezpečnosti; • vede rozvojové projekty ve všech fázích – inicializace, plánování, realizace, monitoring a reporting, prezentace výstupů, vyhodnocení a uzavření; zpracovává časový a finanční plán realizace projektu; má odpovědnost za realizaci projektu v souladu se schváleným časovým harmonogramem a rozpočtem; vede projektovou dokumentaci; • řídí procesy zřízení služeb včetně sledování a reportování dodržování časového harmonogramu, odpovídá za zřízení služby ve sjednaném termínu a kvalitě;

	• účastní se jednání s pracovníky Objednatele; • zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem; • koordinuje a řídí implementaci projektových řešení vč. vedení dokumentace v oblasti kybernetické bezpečnosti.
Manažer kybernetické bezpečnosti	Manažer kybernetické bezpečnosti je osoba, která: • zajišťuje povinnosti bezpečnostní role vycházející ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti); • poskytuje odborné konzultace v oblasti systému řízení bezpečnosti informací/kybernetické bezpečnosti; • zajišťuje prosazování bezpečnosti informací v rámci organizace objednatele; • metodicky řídí procesy systému řízení bezpečnosti; • zajišťuje tvorbu, aktualizaci a realizaci kybernetické bezpečnostní politiky a další dokumenty organizace; • koordinuje tvorbu bezpečnostního konceptu organizace, konceptu plánu obnovy, havarijních plánů a ostatních dílčích konceptů a systémových bezpečnostních pravidel, jakož i vydávání doplňujících pravidel a vodítek celkové kybernetické bezpečnosti; • provádí iniciaci, sledování a vyhodnocování implementace opatření kybernetické bezpečnosti; • ověřuje a vede vyšetřování kybernetických bezpečnostních událostí a incidentů; • určuje způsoby realizace stanovených bezpečnostních politik; • zpracovává bezpečnostní dokumentaci a procesy; • monitoruje výkonnosti systému řízení bezpečnosti informací a účinnosti bezpečnostních opatření; • zajišťuje zvyšování povědomí zaměstnanců organizace o kybernetické bezpečnosti; • připravuje podklady pro přezkoumání systému řízení bezpečnosti informací vedením organizace; • účastní se jednání s pracovníky Objednatele; • zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem; • provádí analýzu, sběr, dekompozici a syntézu získaných informací a navrhuje implementaci bezpečnostního monitoringu.
Manažer řízení rizik KB	Manažer řízení rizik je osoba, která: • identifikuje a hodnotí aktiva a rizika kybernetické bezpečnosti; • posuzuje jednotlivé hrozby, dopady a zranitelnosti působící na bezpečnost organizace; • vytváří dokumentaci k provedené analýze rizik; • připravuje a předkládá návrhy k mitigaci rizik dle pokynů Objednatele; • účastní se jednání s pracovníky Objednatele; • zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem; • vykonává metodickou a konzultační činnost v oblasti analýzy a správy rizik.
Bezpečnostní administrátor ICT	Bezpečnostní administrátor ICT je osoba, která:

	• spolupracuje s administrátory ICT a bezpečnostními správci IS při připojování zdrojových logů do SIEM; • kontroluje konfiguraci bezpečnostních prvků nasazených v ICT; • provádí kontroly aktiv objednatele; • spolupracuje při tvorbě bezpečnostní dokumentace ICT; • podílí se na definici use-case pro jednotlivé ICT; • spolupracuje na analýze, sběru, dekompozici a syntéze získaných informací a navrhuje implementaci bezpečnostního monitoringu. • Zajišťuje testování bezpečnosti řešení
Organizátor vzdělávacích aktivit KB	Organizátor vzdělávacích aktivit KB je osoba, která: • poskytuje konzultace k tvorbě návrhu ročního plánu budování bezpečnostního povědomí; • poskytuje konzultace k tvorbě návrhů individuálních plánů vzdělávání v dané oblasti pro zaměstnance zastávající bezpečnostní role včetně certifikací; • účastní se jednání s pracovníky Objednatele; • zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem; • poskytuje konzultace k vedení evidence záznamů o vzdělávání a přípravě návrhu roční zprávy o budování bezpečnostního povědomí.
Administrátor UNIX	V oblasti serverů s operačními systémy Unix/Linux/VMWare zajišťuje instalaci a konfiguraci HW/SW komponent, správu a údržbu provozovaného HW/SW, administraci a zálohování operačních systémů, řešení incidentů a problémů, zavádění změn, přípravu podkladů pro reporting dodržování SLA a pro technický rozvoj.
Administrátor Microsoft technologií (MS)	V oblasti serverů s operačními systémy Windows a dalších Microsoft technologií zajišťuje instalaci a konfiguraci HW/SW komponent, správu a údržbu provozovaného HW/SW, administraci a zálohování operačních systémů, řešení incidentů a problémů, zavádění změn, přípravu podkladů pro reporting dodržování SLA a pro technický rozvoj.
Administrátor databáze (DB)	Instaluje, spravuje a provádí údržbu DB, podílí se na návrhu nové a změn stávající DB, navrhuje, realizuje a testuje postupy zálohování a obnovy DB, podílí se na návrhu, realizaci a testech monitoringu DB, provádí upgrade DB, vytváří a aktualizuje dokumentaci DB systémů, zakládá DB uživatele a přiděluje přístupy, instaluje aplikace do DB.
Administrátor správy a zálohování (SAZ)	Instaluje, konfiguruje, spravuje a provádí údržbu zálohovacích technologií, sleduje a řeší problémy a poruchy příslušných HW a SW komponent, zajišťuje podklady pro reporting o dodržování SLA.
Administrátor síťových technologií (NET)	Spravuje síťové a další podpůrné technologie v oblasti LAN/WAN, zajišťuje údržbu síťových komponent, navrhuje změny síťové architektury a realizuje je, podílí se na tvorbě LAN/WAN strategie, navrhuje a implementuje monitoring datových sítí, řeší incidenty, problémy a změnové požadavky v oblasti síťové infrastruktury a navrhuje a zajišťuje její další rozvoj. Jedná se zejména o: • návrh sítě a jejích komponent s ohledem na funkční, výkonové, bezpečnostní a spolehlivostní požadavky, • údržba a správa počítačových sítí a souvisejících výpočetních prostředí, včetně hardware, systémového a aplikačního software a souvisejících konfigurací, • monitorování síťového provozu, aktivity na síti, kapacity a jejich využívání pro zajištění optimálního výkonu sítě,

	• posouzení a doporučování opatření ke zlepšení výkonu, bezpečnosti a spolehlivosti sítě, • poskytování specializovaných znalostí na podporu řešení problémů sítě, • instalace, konfigurace, testování, údržba a správa nových segmentů sítí, softwarových aplikací, serverů a pracovních stanic, • dokumentace provozu sítě, evidence a analýzy diagnóz a řešení síťových selhání, rozšíření a modifikace sítě a pokyny pro údržbu, • zajištění souladu software asset managementu a konfiguračního managementu.
Administrátor aplikace	Spravuje přidělenou aplikaci dle postupů specifikovaných u konkrétní aplikace. • zajišťuje běžnou administraci aplikací • zajišťuje dostupnost aplikací dle SLA • poskytuje konzultace v oblasti správy aplikací • poskytuje konzultace v oblasti ladění výkonnosti a návrhu aplikace • instaluje aplikační software a jeho záplaty • navrhuje, realizuje a testuje zálohování a obnovu aplikací • podílí se na návrhu, realizaci a testech monitoringu aplikací • vytváří a aktualizuje dokumentaci aplikací • vytváří uživatelské účty, přiděluje jim přístupová oprávnění a role v aplikacích • spolupracuje s externími dodavateli aplikačního SW • navrhuje, aplikuje a testuje bezpečnostní pravidla nad aplikacemi • vede řádnou evidenci a sleduje stav určených SW komponent
IT analytik / IT architekt	Analyzuje potřeby a požadavky na ICT infrastrukturu a navrhuje technický způsob jejich řešení s využitím portfolia standardních HW/SW komponent, provozně adoptovaných technologických znalostí a zavedených sdílených služeb pro dosažení efektivity a nákladové optimalizace při jejich realizaci i v následném provozu, zpracovává technické projekty a vytváří podklady pro jejich implementaci, navrhuje směry dalšího rozvoje a využití nových technologií a poskytuje odborné konzultace v oblasti ICT technologií a technické architektury.
Business analytik	Poskytuje konzultační a analytické činnosti, včetně aktivit souvisejících s testováním na základě zadání. Mezi analytické činnosti patří zejména definice business požadavků na rozvoj a podporu informačních systémů, informačních a komunikačních technologií, vývoj nových technologických postupů. V oblasti testování zajišťuje tvorbu a zavedení testovacích strategií, test analýz včetně přípravy test cases, test suits a testovacích skriptů. Definuje požadavky na testování, připravuje plán a harmonogram testování, typy testů a jejich metriky. Pro fázi ukončení testů připravuje metriky pro hodnocení testů, vstupy a výstupy z testování. Realizuje a řídí vykonání všech připravených testů. V oblasti konzultací poskytuje odborné výstupy uvedeným oddělením v pozici žadatelů o tuto službu. Konzultace jsou poskytovány s ohledem na aktuální trendy na trhu na poli business analýz a s ohledem na usnadnění rozhodování v rámci daného týmu.
Manažer služeb	Řídí dodávku poskytovaných služeb v dohodnuté kvalitě, tj. v souladu se smluvně zakotveným SLA, je primárním kontaktem zákazníka pro

	řešení jeho požadavků a potřeb, reportuje zákazníkovi průběh plnění služeb a dodržování SLA, projednává se s ním akceptaci plnění a připravuje podklady pro fakturaci, působí jako konzultant zákazníka a podílí se na přípravě a realizaci projektů zavedení nových či rozšiřování stávajících služeb.
Projektový manažer	Zajišťuje řízení projektu s cílem dodání všech projektových výstupů v požadovaném rozsahu, kvalitě a termínech a při dodržení schváleného rozpočtu projektu a minimalizaci rizik, sestavuje plán projektu, vede projektový tým, ukládá úkoly jeho členům a kontroluje jejich plnění, zajišťuje tvorbu projektových dokumentů, koordinuje práci projektových týmů, určuje pravidla jejich komunikace a spolupráce, reportuje stav plnění projektu a zajišťuje identifikaci a řízení jeho rizik vč. včasné eskalace.
Procesní manažer	Navrhuje podnikové procesy pro zajištění jejich souladu s požadavky norem ISO, především ISO 20000 a ISO 27001; definuje dokumentaci procesů ITMS; navrhuje přiměřené zdroje pro běh procesů nutné k dosažení potřebných standardů kvality; vytváří podnikové procesní mapy; navrhuje změny procesů za účelem naplnění nových potřeb; provádí analýzy a poskytuje konzultace v oblasti procesního řízení ITSM (zejm. dle metodologie ITIL), procesní architektury ITSM a procesních standardů.
Správce licencí	Zpracovává žádostí o udělení/změnu a zrušení licence, iniciuje nákup potřebných licencí, vede evidenci pořízených licencí a jejich užití, zajišťuje související následnou agendu včetně pravidelných kontrol pro zajištění efektivity využití licencí a licenční čistoty, poskytuje konzultace žadatelům o udělení/změnu a zrušení licence.
Datový analytik	Datový analytik je osoba, která: • se podílí na vývoji datových modelů, na tvorbě a správě reportů • je odpovědný za datové zdroje, jejich přípravu a zpracování; • připravuje datové výstupy dle požadavků; • systematicky pracuje na zlepšování reportů, jejich automatizaci a optimalizaci; • získává data z primárních systémů; • rozvíjí datový model; • spolupracuje s testery, architekty, business analytiky; • odpovídá za ETL procesy.

Role	v Kč bez DPH za 1 MD	DPH	v Kč včetně DPH za 1 MD
Analytik kybernetické bezpečnosti	13 100,00	2 751,00	15 851,00
Architekt kybernetické bezpečnosti	16 900,00	3 549,00	20 449,00
Manažer kybernetické bezpečnosti	13 800,00	2 898,00	16 698,00
Manažer řízení rizik KB	12 100,00	2 541,00	14 641,00
Organizátor vzdělávacích aktivit KB	11 400,00	2 394,00	13 794,00
Manažer rozvoje služeb KB	14 200,00	2 982,00	17 182,00
Bezpečnostní administrátor ICT	12 600,00	2 646,00	15 246,00
Aplikační administrátor	11 400,00	2 394,00	13 794,00
Datový analytik	11 200,00	2 352,00	13 552,00
Administrátor UNIX	13 400,00	2 814,00	16 214,00
Administrátor Microsoft technologií (MS)	12 300,00	2 583,00	14 883,00

SPCSS
Státní pokladna
Centrum sdílených služeb

Příloha č. 2 Katalog rolí a ceník rolí

Role	v Kč bez DPH za 1 MD	DPH	v Kč včetně DPH za 1 MD
Administrátor databáze (DB)	14 600,00	3 066,00	17 666,00
Administrátor správy a zálohování (SAZ)	13 600,00	2 856,00	16 456,00
Administrátor síťových technologií (NET)	13 200,00	2 772,00	15 972,00
IT analytik / IT architekt	14 200,00	2 982,00	17 182,00
Manažer služeb	12 900,00	2 709,00	15 609,00
Projektový manažer	12 900,00	2 709,00	15 609,00
Procesní manažer/architekt	11 400,00	2 394,00	13 794,00
Správce licencí	10 200,00	2 142,00	12 342,00
Business analytik	15 000,00	3 150,00	18 150,00

Specifické služby v oblasti kybernetické bezpečnosti na vyžádání mohou být poskytovány **pro konkrétní aplikace** Objednatele na základě písemného vyžádání oprávněné osoby Objednatele. Konkrétní definice služby bude vytvořena pracovníky SPCSS na základě analýzy požadavků Objednatele s využitím především popisu jednotlivých podslužeb kybernetické bezpečnosti uvedeném v této Příloze č. 3 Smlouvy.

Výstupem analýzy bude nový katalogový list služby, který bude formou změnového řízení a uzavřením dodatku ke Smlouvě zařazen do katalogu služeb, který je Přílohou č. 1 Smlouvy.

Běžné provozní **služby v oblasti kybernetické bezpečnosti pro infrastrukturní služby jsou zahrnuty do služeb popsaných v jednotlivých katalogových listech katalogu služeb**, které jsou Přílohou č.1 Smlouvy

Jednotlivé podslužby kybernetické bezpečnosti, ze kterých na základě analýzy Objednatel navrhuje podle požadavku Objednatele specifické služby, a jejich popis jsou uvedeny v následujících kapitolách.

Následující tabulka uvádí přehled podslužeb kybernetické bezpečnosti využitelných pro jednotlivé aplikace Objednatele. V jednotlivých **katalogových listech** budou definovány specifické služby pro konkrétní informační systémy.

Specifické vyžádané služby kybernetické bezpečnosti mohou být poskytovány v prostředí „on-premise, cloud, hybrid."

V rámci poskytování všech Podslužeb si Dodavatel vyhrazuje právo na plánované odstávky celého nebo částí systému z důvodu údržby jak samotného systému, tak infrastruktury a datové konektivity Dodavatele. Dodavatel se zavazuje plánované práce s vlivem na dostupnost Podslužeb soustředit do jednoho termínu tak, aby byly poskytované Služby ovlivněna co nejméně.

Plánované odstávky jsou, pokud možno, soustředěny do servisních oken, která jsou každý čtvrtek v čase 19:00 až 24:00, pokud není v katalogovém listu služby uvedeno jinak. Ve výjimečných případech jsou odstávky Podslužeb ohlašovány a realizovány i mimo tato servisní okna. Doba odstávky, která byla předem řádně ohlášena se nezapočítává do nedostupnosti Podslužeb. Za ohlášení se považuje informování určených osob Objednatele e-mailem, a to minimálně 24 h před zahájením mimořádné odstávky.

Detailní popis podslužeb kybernetické bezpečnosti je uveden v následujících kapitolách této Přílohy č.3 Smlouvy.

Podslužby kybernetické bezpečnosti
1. Bezpečnostní monitoring
2. Analýza rizik
3. Správa účtů
4. Vulnerability management
5. Penetrační testy
6. Kompetenční centrum KB

1. BEZPEČNOSTNÍ MONITORING

Katalogový záznam

Název	Bezpečnostní monitoring
Principy stanovení ceny	EPS (events per second), Instance DB
Dostupnost (roční)	99,5 %
Provozní doba	24x7

1.1 Popis služby

Služba Bezpečnostní monitoring je ucelené řešení pro pokrytí potřeb bezpečnostní problematiky v souladu s platným právním řádem. Bezpečnostní monitoring je prováděn dohledovým pracovištěm a expertním týmem SOC SPCSS. Služba Bezpečnostní monitoring je poskytována v nepřetržitém režimu 24x7 a zahrnuje sběr informací, jejich třídění, korelaci, kategorizaci, analýzu a archivaci. Použité technologie SPCSS a nástroje SPCSS umožňují detekci známých bezpečnostních útoků, podezřelého chování a anomálií.

V rámci Služby Bezpečnostní monitoring je také poskytován proces zvládání kybernetických bezpečnostních incidentů včetně přípravy podkladů pro příslušné orgány v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti (dále také „ZoKB") v platném znění a podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále také „VoKB"), případně na základě dohody Smluvních stran.

Služba Bezpečnostní monitoring pokrývá vybrané povinnosti definované zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění, resp. vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti. Specifika dle klasifikace informací a povahy spravovaného systému (jako KII, VIS) jsou ze strany Objednatele určeny prováděcí smlouvou.

Jedná se o tato opatření:

- § 14 Zvládání kybernetických bezpečnostních událostí a incidentů
- § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
- § 23 Detekce kybernetických bezpečnostních událostí
- § 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí
- § 31 Kategorizace kybernetických bezpečnostních incidentů
- § 32 Forma a náležitosti hlášení kybernetických bezpečnostních incidentů

Služba Bezpečnostní monitoring je realizována v rozsahu aktiv, definovaných Objednatelem v příslušných Prováděcích smlouvách. Služba je poskytována za využití nástrojů a prostředků ve vlastnictví SPCSS, které zprostředkovávají realizaci sběru, vyhodnocování a uchovávání logů.

Předmětem Služby Bezpečnostní monitoring je nepřetržitý bezpečnostní monitoring v režimu 24x7 definovaných aktiv Objednatele.

Typy záznamů, se kterými Služba Bezpečnostní monitoring pracuje, jsou zejména:

- logy operačních systémů;
- logy aplikací;
- logy síťových prvků;
- logy infrastruktury a virtualizačního prostředí;
- NetFlow.

V rámci Služby je určeným pracovníkům Objednatele umožněn přístup do prostředí SIEM, kde mohou sledovat aktivity, které generují monitorované systémy. Náhled neslouží pro vyšetřování KBU, KBI ani pro analýzy.

V rámci služby je možné využít doplňující volitelné části. Volitelné Služby nemohou být poskytovány samostatně. Podmínkou pro poskytování volitelných služeb je využití hlavní Služby Bezpečnostní monitoring. Volitelná Služba Virtuální kolektor pro bezpečnostní monitoring je určena pro monitorované aktivum Objednatele. Volitelná Služba Bezpečnostní monitoring databází pomáhá se zabezpečením citlivých dat v prostředí databází a datových skladů. Bezpečnostní monitoring databází se skládá ze třech částí – kolektor (jedná se o kolektor speciálně určený pro monitoring databází), virtuální agregátor (řešení je primárně určeno pro centrální správu všech instancí Bezpečnostního monitoringu databází, které jsou na něj připojeny) a nástroj pro analýzu a ochranu dat v databázích.

2. ANALÝZA RIZIK

2.1 Popis služby

Analýza rizik je poskytována prostřednictvím role Manager řízení rizik KB.

Služba analýzy rizik spočívá v provedení vstupní analýzy rizik systému VIS dle zvolené metodiky Dodavatele a s využitím příslušných nástrojů. U takto analyzovaných rizik lze následně sjednat i jejich správu. Analýza rizik prováděná na základě významné změny systému požadované ze strany Objednatele není součástí této služby a její realizace může být vykonána pouze na základě dohody Smluvních stran postupem dle Rámcové smlouvy. Analýza rizik prováděná na základě významné změny systému, která není vyvolána na základě požadavku Objednatele, je prováděna v souladu s ust. § 11 odst. 2 písm. b) VoKB.

Obsahem Služby je identifikace a ohodnocení aktiv a rizik pro dosažení souladu prvků VIS s požadavky ZoKB a VoKB.

Součástí dodávky Služby jsou:

- Definice metodiky pro hodnocení rizik Dodavatele;
- Vypracování výstupní dokumentace dle ZoKB a VoKB:
  - Zpráva o hodnocení aktiv a rizik;
  - Plán zvládání rizik;
  - Prohlášení o aplikovatelnosti.

3. SPRÁVA ÚČTŮ

Katalogový záznam

Název	Správa účtů
Principy stanovení ceny	uživatel, KS
Dostupnost (roční)	99,5 %
Provozní doba	24x7

3.1 Popis služby

Služba je poskytována pro správu běžných a privilegovaných účtů.

Privilegované účty disponují prakticky neomezeným přístupem k systémům a lze díky nim s těmito systémy manipulovat, tím se stávají významným bezpečnostním rizikem týkající se všech systémů. Rizika se týkají operačních systémů, databází, síťových prvků až po komplexní informační systémy distribuované jako produkt, nebo vyvinuté na míru. Specifické nároky jsou na systémy identifikované jako „Významný informační systém" nebo „Kritická informační infrastruktura" v rámci zákona č. 181/2014 Sb., zákon o kybernetické bezpečnosti, kdy je nezbytné jako opatření zavést správu přístupu k privilegovaným účtům a monitoring veškeré aktivity účtů s vazbou na konkrétní osobu, která jím právě disponuje. Využití této Služby Správa privilegovaných účtů se doporučuje i pro ostatní pro Objednatele významné informační systémy. Řešení je poskytováno v režimu vysoké dostupnosti.

Služba je z technologického hlediska složena z:

- Jumpserver EKRAN, přes který se přistupuje ke spravovaným aktivům;

- aplikační část EKRAN, která je oddělena od Jumpserveru a umožňuje granulární nastavení správy účtů, přístupů a politik alertingu a logování stejně jako nastavení session recordingu.

Proces:

Zákazník může kontrolovat přístupové údaje, konfiguraci, nahrávky přihlášením k webovému portálu EKRAN. Rozsah oprávnění zákazníka k přístupu k nahrávkám je definován při zavedení služby. Přístup dodavatelů může definovat zákazník, nebo se provede v rámci implementace služby. Alerting si může zákazník definovat, jak potřebuje ve webovém portálu EKRAN, nebo formou tiketu v SD na dodavatele.

Oprávnění jsou řízena definováním rolí a přístupové politiky v rámci systému EKRAN. Nahrávání session recordingu lze nastavit u zákazníka a dodavatel tak nemusím mít práva pro zobrazení.

Služba Správy privilegovaných účtů obsahuje tyto oblasti:

- Řízení přístupu privilegovaných účtů – kontrola přístupu k informačnímu systému pomocí privilegovaných účtů dle požadovaného rozsahu (např. infrastruktura, aplikační úroveň). Týká se to všech účtů, které budou přistupovat skrze Jumpserver EKRAN.
- Session Recording – zaznamenávání aktivit privilegovaných účtu včetně nahrávek obrazovek a stisků kláves (key-logging). Stisk kláves je monitorován pouze v případě, že je využita nativní aplikace Ekran.;
- Password Management – zajišťuje centrální správu účtů se zabezpečeným úložištěm hesel a správou přístupů k těmto účtům;

Služba Správa privilegovaných účtů pokrývá vybrané povinnosti definované zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění, resp. vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti. Specifika dle klasifikace informací a povahy spravovaného systému (jako KII, VIS) budou ze strany Objednatele určeny Prováděcí smlouvou.

Jedná se o tyto opatření:

- § 19 Správa a ověřování identit;
- § 20 Řízení přístupových oprávnění.

Služba Správa privilegovaných účtů se skládá z volitelných komponent Identity Management a Session Recording a Password Management uvedených v příslušných Prováděcích smlouvách.

4. VULNERABILITY MANAGEMENT

Katalogový záznam

Název	Vulnerability management
Principy stanovení ceny	Rozsah scanované aplikace nebo informačního systému, případně infrastruktury mimo SPCSS, vypořádání nálezů ze scanů zranitelností

4.1 Popis služby

Služba Vulnerability management je podpůrné řešení v minimalizaci výskytu zranitelností v aplikacích a informačních systémech definovaných příslušnými Prováděcími smlouvami a slouží jako nástroj i pro naplnění legislativních požadavků podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále také „VoKB").

Předmětem Služby Vulnerability management je skenování zranitelností probíhající jedenkrát měsíčně nebo manuálním Ad-hoc skenem (např. při zveřejnění kritické zranitelnosti). Služba Vulnerability management je realizována v rozsahu definovaných aktiv Objednatelem.

Služba Vulnerability management slouží k zjišťování zranitelností prostřednictvím řešení, kdy na sledovaném zařízení není instalován žádný agent, který by komunikoval s nástrojem pro skenování. Jedná se tedy o bezagentní řešení. Tento způsob snižuje nároky na nasazení i poskytování Služby Vulnerability management. Řešení také umožňuje detailnější analýzu při

využití systémového účtu, který skenovací nástroj využije proto, aby mohl provádět kontrolu přímo na daném aktivu.

Skenování zranitelností v rámci Služby Vulnerability management probíhá dle metodiky NIST.

Služba Vulnerability management snižuje nároky na zdroje Objednatele pro včasnou kontrolu a ověřování zranitelností. Součástí Služby je poskytování přehledného reportingu.

Podslužbu Vulnerability management lze provozovat v perimetru Objednatele, i z prostředí SPCSS.

Služba Vulnerability management je podpůrným prostředkem pro částeční či úplné naplnění povinností definovaných zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, v platném znění, resp. Vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti. Vulnerability management obsahuje obecný výčet požadavků VoKB, pro jejichž naplnění Objednateli Služba Vulnerability management poskytuje informace. Specifika dle klasifikace informací a povahy spravovaného systému (jako KII, VIS) jsou ze strany Objednatele určeny prováděcí smlouvou.

Jedná se o tyto paragrafy VoKB:

- § 5 Řízení rizik;
- § 10 Řízení provozu a komunikací;
- § 11 Řízení změn;
- § 14 Zvládání kybernetických bezpečnostních událostí a incidentů;
- § 28 Průmyslové, řídicí a obdobné specifické systémy.

Služba Vulnerability management nepokrývá výše zmíněné ustanovení VoKB v plném rozsahu, ale výstupy Služby Vulnerability management jsou využívány při realizaci jednotlivých organizačních a technických opatření v rámci SŘBI Objednatele.

Jednotlivé kroky poskytování Služby Vulnerability management:

- příprava a průběžná úprava skenovacích scénářů;
- počáteční inicializační sken;
- periodický sken;
- kontrolní sken nebo Ad-hoc sken prováděný na vyžádání;
- pravidelná zpráva o stavu Služby dle tohoto dokumentu.

Podslužbu Vulnerability management lze využít na:

- operační systémy (Microsoft Windows, UNIX, Cisco, Android, Linux, Apple, Macintosh, Apple iOS);
- webové aplikace, kde jsou využity moduly dle OWASP a CWE;
- zranitelnosti i malware v aplikacích a produktech známých výrobců;
- nejpoužívanější databázové platformy.

5. PENETRAČNÍ TESTY

Katalogový záznam

Název	Penetrační testy
Principy stanovení ceny	Rozsah provedených penetračních testů aplikace nebo informačního systému, případně infrastruktury mimo SPCSS, vypořádání nálezů z penetračního testování

5.1 Popis služby

Služba Penetrační testy analyzuje do jaké míry je konkrétní systém odolný proti útoku, kde jsou jeho slabá místa a jak je nejlépe odstranit. Tato Služba je také prováděna za účelem zjištění slabin v zabezpečení systémů definovaných příslušnými Prováděcími smlouvami, konfiguračních chyb a bezpečnostních mezer. Pro realizaci Služby je používána uznávaná metodika Penetration Testing Execution Standard (PTSE).

Výsledkem Služby Penetrační testy je přehled, čeho by mohl dosáhnout případný útočník při reálném útoku.

Aktivní testování se podle této přílohy provádí zásadně na základě vyžádání Objednatelem a písemného souhlasu dalších osob, kterých by se mohlo testování nějak dotknout. Před započetím vlastního testování je nutné stanovit jasné podmínky testování, tedy určení času, cílů testu (adresy, domény, emaily, osoby).

Služba Penetrační testy je navržena tak, aby Objednateli pokryla celou škálu činností vyplývajících z povinnosti definovaných zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění, resp. vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti.

§25 Aplikační bezpečnost – Povinná osoba provádí penetrační testy informačního a komunikačního systému se zaměřením na důležitá aktiva, a to před jejich uvedením do provozu a v souvislosti s významnou změnou podle § 11 odst. 3. (Povinná osoba na základě výsledků analýzy rizik rozhoduje o provedení penetračního testování nebo testování zranitelností).

Typy penetračních testů:

- externí penetrační testy, kde se jedná o prověření perimetru na základě přístupu z internetu v rozsahu prověření zabezpečení DMZ, firewallu, serverů jak v DMZ, tak v LAN a web aplikací;
- interní penetrační testy, kde se jedná o řízenou simulaci útoku z vnitřní sítě na servery a aplikace;
- sociální penetrační testy, kde se jedná o prověření dodržování procesů, postupů a bezpečnostních zásad v rámci organizace.

Oblasti penetračních testů určují jejich zaměření a jsou následující. V rámci Služby jsou definovány tyto oblasti:

- penetrační test sítě;
- penetrační test wi-fi sítě;
- penetrační test aplikací;
- penetrační test webu/portálů;
- penetrační test zaměřený na uživatele a hesla;
- penetrační test mobilních zařízení;
- penetrační test pracovních stanic;
- penetrační test serverových technologií.

Služba je realizována následujícími možnými způsoby:

- Double blind;
- Blind;
- Black box;
- Gray box;
- White box;

Služba je poskytována, pro oblast penetračních testů ve dvou variantách:

- základní – test zaměřený na odhalení nejzávažnějších zranitelností;
- detailní – test zaměřený na komplexní bezpečnostní audit.

6. KOMPETENČNÍ CENTRUM KB

Katalogový záznam

Název	Kompetenční centrum KB
Principy stanovení ceny	Počet dokumentů evidovaných v Nástroji

6.1 Popis služby

Služba Kompetenční centrum kybernetické bezpečnosti zahrnuje podporu činností vyplývajících pro povinné osoby Objednatele z právních předpisů (zejména zákon č. 181/2014 Sb., o kybernetické bezpečnosti, resp. vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti).

Služba Kompetenční centrum KB je určena jako **odborná administrativní podpora** v oblasti informační a kybernetické bezpečnosti pro Objednatele. Služba Kompetenční centrum KB zajišťuje podporu vedení a správy systému řízení bezpečnosti informací (dále také „**SŘBI**") včetně administrace s využitím sofistikovaného nástroje pro podporu systému řízení bezpečnosti informací (dále také „**Nástroj**"), který slouží jako platforma pro tvorbu, aktualizaci a sjednocení přístupu k povinné dokumentaci, včetně nastavení workflow, evidenci a reporting činností a agend. Podporu poskytují odborníci SPCSS.

Na základě konkrétních dodaných podkladů od Objednatele je Poskytovatelem udržována aktuální evidence klíčové agendy kybernetické bezpečnosti v Nástroji, čímž je zajištěn přehled Objednatele o povinných činnostech v rámci dotčené oblasti SŘBI.

Dokumentem, pro potřeby Služby Kompetenční centrum KB, je myšlen každý v Nástroji vytvořený nebo naimportovaný soubor (pdf, doc, xls, jpg či jiného kompatibilního formátu) do modulu Dokumentace v Nástroji. Jedná se zejména o dokumenty obsahující interní předpisy (směrnice, metodiky a jejich přílohy) a dokumentaci SŘBI.

Za dokument v té části Dokumentace SŘBI Objednatele, která obsahově odpovídá výčtu dle Přílohy č. 5 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, je vždy považován nejméně každý bod (1.1 až 1.23 a 2.1 až 2.11) dle Přílohy č. 5 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, tj. Dokumentace SŘBI Objednatele v této části zahrnuje vždy nejméně 34 dokumentů.

SPCSS využívá Nástroj jako nedílnou součást Služby Kompetenční centrum KB. Implementace dat Objednatele probíhá na základě analýzy stávajícího stavu SŘBI u Objednatele a jeho individuálních požadavků a v souladu s legislativou. Dodávka licence Nástroje není předmětem Služby Kompetenční centrum KB. Nástroj je umístěn v prostředí SPCSS, které poskytuje vysokou kvalitu služeb a vysokou úroveň zabezpečení (Bezpečné datové centrum).

Metodická Podpora Objednatele

Součástí Služby Kompetenční centrum KB je také metodická podpora Objednatele v oblasti informační a kybernetické bezpečnosti. Podporu poskytují odborníci SPCSS na vyžádání Objednatele.

Metodická podpora se soustřeďuje zejména na povinnosti vyplývající z oblasti SŘBI a informační a kybernetické bezpečnosti Objednatele.

Výstupy z Metodické podpory SŘBI Objednatele jsou zapracovány formou vstupů do Nástroje pro podporu řízení SŘBI nebo dle požadavku Objednatele.

Volitelné součástí Služby Kompetenční centrum

Volitelné součástí Služby Kompetenční centrum nemohou být poskytovány samostatně. Podmínkou pro poskytování volitelných služeb je využití hlavní Služby Kompetenční centrum kybernetické bezpečnosti.

Volitelná služba Administrativní podpora v oblasti Ochrany osobních údajů dle ZoKB. Tato Volitelná služba nezahrnuje právní služby v oblasti Ochrany osobních údajů.

Volitelná Služba Podpora v oblasti budování bezpečnostního povědomí v organizaci v souladu s povinnostmi uloženými ZoKB/VoKB včetně podpůrné platformy pro realizaci vzdělávání formou e-learningových kurzů.

ŘÍZENÍ PROVOZU

Tato příloha popisuje metodiku a procesy řízení Služeb bezpečného datového centra (dále jen „Služeb") ve spolupráci Poskytovatele (SPCSS) a Objednatele (MF).

Metodika řízení provozu Služeb vychází ze Směrnice SPCSS pro řízení provozu služeb a ze Směrnice pro přípravu a poskytování služeb, upravené pro řízení spolupráce při poskytování a akceptaci Služeb.

1. ŘÍDÍCÍ ORGÁNY PROVOZU

1.1 Řídící komise

Řídicí komise (dále jen „**ŘKO**") je nejvyšším řídicím orgánem a nejvyšší eskalační autoritou pro veškeré záležitosti provozu Služeb. Členy ŘKO jsou zástupci MF a SPCSS na vyšší manažerské úrovni, jmenovaní každou ze Smluvních stran po podpisu Smlouvy. Členové ŘKO ze strany MF i SPCSS musí být vybaveni potřebnými kompetencemi rozhodovat v zásadních otázkách, musí mít možnost alokovat potřebné zdroje a musí mít možnost prosadit rozhodnutí v rámci příslušné Smluvní strany. Na jednání ŘKO mohou být na žádost zástupců MF či zástupců SPCSS přizváni s poradním hlasem další externí odborníci nebo zástupci dalších stran.

1.2 Manažeři Služeb a TPP

Tato kapitola definuje hlavní role a orgán řízení provozu na úrovni procesů popsaných v této příloze Smlouvy.

Manažeři Služby za MF a SPCSS jsou oprávněné osoby ve věcech řízení provozu služeb. Manažeři Služeb MF a SPCSS zodpovídají za řádné plnění povinností svých Smluvních stran v rámci provozu. Připravují podklady k rozhodování ŘKO.

Vzhledem k předpokládanému množství služeb bude na obou stranách více než jeden manažer služby. ŘKO schválí dokument „Nominace provozních týmů", ve kterém budou pro každou ze služeb z katalogu služeb (Příloha č.1 Smlouvy) jmenováni manažer služby za MF a za SPCSS.

Manažer služby za SPCSS zpracovává 1x měsíčně Zprávu o úrovni a rozsahu poskytovaní služby v souladu se Smlouvou a předkládá ji Manažerovi služby za MF k akceptaci.

Bezpečnostní manažeři Služeb za MF a SPCSS odpovídají za bezpečnost provozu služby. Tyto role jsou rovněž stanoveny v rámci dokumentu „Nominace provozních týmů".

Tým přípravy a poskytování služeb (dále jen „**TPP**"):

- je složen ze zástupců SPCSS, MF a případně i dalších třetích stran ve smluvním vztahu s MF nebo SPCSS;
- řeší aktuální problémy jak ve fázi přípravy Služeb, tak ve fázi poskytování Služeb;
- identifikuje možná rizika;
- řídí a monitoruje kvalitu poskytování Služby s ohledem na identifikované problémy a rizika. Analyzuje a posuzuje rizika a, pokud tak rozhodne ŘKO, vede Registr rizik provozu. Projednává a schvaluje návrhy na mitigaci identifikovaných rizik s cílem jejich minimalizace a jeho dopadů;
- zajišťuje mitigaci rizik;
- identifikuje a projednává změny v rozsahu poskytované Služby, termínů, ceny nebo kvality plnění Služby. Analyzuje dopady změn na Službu a předkládá návrhy ŘKO;
- projednává a předkládá návrhy na optimalizaci a změnu Služby;
- připravuje a aktualizuje EXIT plán.

2. NÁSTROJE ŘÍZENÍ PROVOZU

2.1 Úrovně podpory

Při popisu a řízení Služby jsou používány následující definice úrovně podpory:

- **První úroveň podpory** (Level 1, **L1**, někdy také nazýván "First line" nebo "Front end support") – zajišťuje přímou komunikaci s Objednatelem a uživateli (v definovaném rozsahu), převzetí informací, evidenci požadavků a incidentů v podpůrných nástrojích a prvotní analýzu požadavku nebo incidentu. Odpovídá na jednoduché požadavky na základě znalostní báze nebo na základě stavu aktuálně řešených incidentů. Pokud řešení požadavku převyšuje vědomosti podpory první úrovně, předává požadavek nebo incident vyšší úrovni podpory. V rámci provozních služeb SPCSS je tato úroveň podpory interně realizována prostřednictvím ServiceDesku Poskytovatele.
- **Druhá úroveň podpory** (Level 2, **L2**) – řeší složitější požadavky a incidenty, jejichž řešení ovšem nevyžaduje hluboké znalosti aplikací, systémů nebo SW/HW a přístup ke zdrojovému kódu nebo náhradním dílům.
- **Třetí úroveň podpory** (Level 3, **L3**, v případě HW/SW produktů rovněž nazývána HW/SW maintenance) - řeší nejsložitější požadavky a incidenty, jejichž řešení vyžaduje hluboké znalosti aplikací, systémů nebo SW/HW a přístup ke zdrojovému kódu nebo náhradním dílům. Podpora L3 je zodpovědná za finální vyřešení problému, ať už řešení zahrnuje komunikaci s výrobcem SW produktů, ať jde o opravu nebo výměnu hardwaru, doprogramování kódu nebo instalaci nezbytných programů.

2.2 Service Desk

Service Desk je standardním nástrojem a službou SPCSS pro poskytování podpory a řízení provozních procesů. Service Desk je poskytován MF jako samostatná služba podle samostatné smlouvy (Smlouva o poskytování služby Service Desk) a za podmínek stanovených touto samostatnou smlouvou a bude využit i pro řízení provozu Služby podle této Smlouvy. Service Desk je využíván jako prostředek formalizovaného způsobu komunikace s uživateli a pracovníky podpory provozu MF i třetích stran.

Service Desk bude využíván pro předávání informací o provozních incidentech a požadavcích a sledování postupu jejich řešení. Řešitelé incidentů a požadavků budou pracovat přímo v prostředí Service Desk.

SPCSS je odpovědný za včasný záznam postupu řešení incidentů (v rozsahu jeho odpovědnosti) v Service Desku, v úrovni detailu dostatečné pro spolupráci ostatních účastníků provozu na jejich řešení a pro zpětný audit příčin incidentů a způsobu řešení.

Plnění smluvních SLA parametrů SPCSS podle této Smlouvy souvisejících s řešením incidentů bude vyhodnocováno na základě údajů zaznamenaných v Service Desku.

3. POSTUP ZMĚNOVÉHO ŘÍZENÍ

3.1 Změnový požadavek

Změnový požadavek může vzniknout na straně Objednatele nebo na straně Poskytovatele. Změnový požadavek vznikne v okamžiku, kdy se v průběhu poskytování nebo i ve fázi přípravy Služby vyskytne skutečnost, která může mít vliv na termíny, cenu, rozsah a kvalitu Služeb.

3.2 Posouzení změnového požadavku

TPP Služby požadavek projedná a navrhne ŘKO, zda bude změnový požadavek postoupen k dalšímu zpracování.

3.3 Analýza dopadů a finančních nákladů

TPP provede podrobnou analýzu dopadů zamýšlené změny. Výsledky analýzy zpracuje do změnového požadavku, který bude obsahovat také odhad finančních nákladů zamýšlené změny.

3.4 Rozhodnutí o realizaci změnového požadavku

Na základě doporučení TPP provede ŘKO rozhodnutí o realizaci změnového požadavku.

3.5 Změna smlouvy

Na základě rozhodnutí ŘKO o realizaci změnového požadavku Manažer Služby za SPCSS případně zajistí návrh obsahu a podpis dodatku ke Smlouvě.

3.6 Plán realizace změnového požadavku

Bezprostředně po rozhodnutí ŘKO vytvoří Manažer Služby za SPCSS plán realizace změnového požadavku v souladu se smluvními dokumenty.

ZÁZNAM O POSKYTNUTÍ SLUŽEB

pro katalogový list č. xx dle Přílohy č.1 Smlouvy na služby bezpečného datového centra č. SML2023143

(evid. u Poskytovatele pod č. _____ a u Objednatele pod č. _____)

Vykazované období:	od	do

Obě Smluvní strany potvrzují, že v uvedeném období byla v souladu s výše uvedenou Smlouvou poskytnuta níže specifikovaná Služba v účtovaném množství:

	Cena za v období (Kč)		
	bez DPH	**DPH**	**s DPH**
Celkem			

Jméno a příjmení oprávněné osoby Objednatele	**Jméno a příjmení oprávněné osoby Poskytovatele**
Podpis a datum	Podpis a datum

Státní pokladna Centrum sdílených služeb, s. p.

se sídlem Na Vápence 915/14, Žižkov, 130 00 Praha 3

ZPRÁVA

o úrovni a rozsahu poskytovaných Služeb v období

_____ - _____

dle Smlouvy na služby bezpečného datového centra
(evid. u Poskytovatele pod č. _____ a u Objednatele pod č. _____)

1. Období poskytování služeb

Zahájení poskytování Služeb	Ukončení poskytování Služeb

2. Režim poskytování služeb
3. Popis rozsahu poskytovaných služeb
4. Výkonnostní parametry poskytovaných služeb
5. Řešení závad
6. Servisní zásahy, provozní změny a testování
7. Dostupnost služeb
8. Závažné incidenty
9. Přehled omezení služeb
10. Přílohy
11. Podpisová doložka

Vypracoval		**Schválil**	
Jméno a příjmení:		**Jméno a příjmení:**	
Podpis		**Podpis**	
Datum:		**Datum:**	
Vyjádření Objednatele k poskytování Služeb:			
Za Objednatele			
Jméno a příjmení:			
Podpis			
Datum:			

ZMĚNOVÝ POŽADAVEK

ZPxxx_xxxxx

NÁVRH NA ZMĚNU SLUŽBY (ZP)

Project ID	Zajištění a provoz produkčního prostředí IISSP
Objednatel	
Krátký název ZP	
Datum podání	dd.mm.rrrr
Datum aktualizace ZP	dd.mm.rrrr
Priorita	Nízká / Střední / Vysoká
Předkladatel	Jméno a příjmení, funkce
Zhotovitel	Jméno a příjmení, funkce

1. ZADÁNÍ

1.1 Popis požadované změny

1.2 Dopady na stávající Službu

1.3 Specifikace SW a HW požadavků

1.4 Popis zajištění realizace změny

1.5 Zdůvodnění změny

1.6 Očekávané důsledky

VÝSLEDEK	☒ Dále zpracovávat ☐ Nerealizovat ☐ Přepracovat ☐ Odložit

	Schválil (SPCSS)	**Schválil (MF)**
Jméno	manažer Služby za SPCSS	manažer Služby za MF
Datum		
Podpis		

2. ANALÝZA ZP – TECHNICKÉ ŘEŠENÍ

2.1 Detailní popis řešení

2.2 Popis současného stavu

2.3 Cílový stav

2.4 Realizované činnosti

ID	Činnost	Zodpovědnost
1.		

2.5 Požadovaná součinnost

2.6 Dopady do kvalitativních parametrů poskytované Služby

2.7 Harmonogram realizace

2.8 Rizika

2.9 Cenové ohodnocení pracnosti a nákladů (pokud budou nad rámec Služby)

2.10 Dopady do dokumentace

ID	Název	Popis změny
1.		aktualizace dokumentu

3. SPOLEČNÁ SEKCE

Rozhodnutí

Datum	
Výsledek rozhodnutí	☒ Dále zpracovávat ☐ Nerealizovat ☐ Přepracovat ☐ Odložit
Požadavek na dodatek ke Smlouvě	☒ ANO ☐ Není potřeba

Podpisem oprávněné osoby potvrzujeme, že s návrhem změny výše popsané dle výsledku rozhodnutí souhlasíme. V případě výsledku Realizovat, je možné ihned zahájit práce na implementaci ZP.

V Praze dne:

Objednatel	**Poskytovatel**
Jméno, příjmení:	Jméno, příjmení:
Podpis: _____	Podpis: _____
Manažer Služby Objednatele	Manažer Služby Poskytovatele
Jméno, příjmení:	Jméno, příjmení:
Podpis: _____	Podpis: _____
Zástupce Objednatele v ŘKO	Zástupce Poskytovatele v ŘKO

Výzva č. xx/RRRR k Poskytování odborných rolí

dle Smlouvy na služby bezpečného datového centra č. SML2023143

Identifikační údaje Objednatele	**Identifikační údaje Dodavatele**
Česká republika – Ministerstvo financí se sídlem: Letenská 525/15, 118 10 Praha 1 za níž jedná:nutno doplnit IČO: 00006947 DIČ: CZ00006947 Bank. spojení: Česká národní banka číslo účtu: 3328001/0710 ID DS: xzeaauv	**Státní pokladna Centrum sdílených služeb, s. p.** zapsaný v obchodním rejstříku vedeném Městským soudem v Praze pod sp.zn. A 76922, se sídlem: Na Vápence 915/14, Žižkov, 130 00 Praha 3 zastoupený:nutno doplnit IČO:036 30 919 DIČ:CZ03630919 Bank. spojení:Česká národní banka číslo účtu: 206201/0710 IBAN: CZ65 0710 0000 0000 0020 6201 ID DS:ag5uunk

Termín zahájení Poskytování odborných rolí	DD.MM.RRRR
Termín ukončení Poskytování odborných rolí	DD.MM.RRRR
Název informačního systému	**nutno doplnit**

Podrobná specifikace Poskytování odborných rolí dle Přílohy č. x Smlouvy
název odborné role (nutno doplnit) – nutno doplnit **název odborné role (nutno doplnit)** – nutno doplnit

Název odborné role	název odborné role (nutno doplnit)
Max. počet člověkodní v požadovaném období	**xx člověkodny**
Rozsah a popis požadované činnosti	nutno doplnit
Specifikace výstupů činnosti	• nutno doplnit

Název odborné role	název odborné role (nutno doplnit)		
Max. počet člověkodní v požadovaném období		**xx člověkodny**	
Rozsah a popis požadované činnosti	nutno doplnit		
Specifikace výstupů činnosti	• nutno doplnit		
Schvalovací doložka			
Jméno a příjmení	**Organizace**	**Podpis**	**Datum**
nutno doplnit	Objednatel		Dle elektronického podpisu

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.first.org/tlp/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Podmínky využití poskytnutých informací

Štítek	Podmínky použití
TLP: RED	Informace není určena pro jiné než určené osoby (určuje původce); poskytnutí informace dalším subjektům ze strany příjemce lze učinit pouze s předchozím souhlasem původce informace.
TLP: AMBER	Informaci je možné sdílet pouze s omezeným okruhem osob (určuje původce); příjemci mohou sdílet tyto informace pouze s členy své organizace a s dodavateli nebo zákazníky, kteří nezbytně potřebují tyto informace znát, aby se chránili nebo zabránili vzniku další škody; původce informace může rozsah sdílení dále omezit.
TLP: GREEN	Informace je určena k omezenému zveřejnění; omezeno na komunitu (organizace příjemce a další partnerské subjekty příjemce informace), avšak nikoliv s využitím veřejně dostupných komunikačních kanálů; příjemce nesmí informaci šířit mimo určenou komunitu (určuje původce).

TLP: WHITE	Zveřejnění informace není omezeno; tímto ustanovením není dotčeno omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran.

Výkaz

dle Smlouvy BDC 2024+

Vykazované období:	od DD.MM.RRRR	do DD.MM.RRRR

Název role	Cena za člověkoden v Kč bez DPH	Člověkohodiny	Člověkodny
nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
	bez DPH v Kč	**DPH v Kč**	**včetně DPH v Kč**
Cena celkem	nutno doplnit	nutno doplnit	nutno doplnit

Dne DD.MM.RRRR akceptovány práce odvedené nutno doplnit v období od DD.MM.RRRR do DD.MM.RRRR v rozsahu **nutno doplnit člověkodnů**.

ID	Název přílohy	Příloha
nutno doplnit	nutno doplnit	Viz dále v Příloze č. x až č. x; (strana č. x až strana č. x tohoto dokumentu)

Schvalovací doložka			
Jméno a příjmení	**Organizace**	Podpis	**Datum**
nutno doplnit	Dodavatel		dle elektronického podpisu
nutno doplnit	Dodavatel		dle elektronického podpisu
nutno doplnit	Objednatel		dle elektronického podpisu
nutno doplnit	Objednatel		dle elektronického podpisu

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.first.org/tlp/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Podmínky využití poskytnutých informací

Štítek	Podmínky použití
TLP: RED	Informace není určena pro jiné než určené osoby (určuje původce); poskytnutí informace dalším subjektům ze strany příjemce lze učinit pouze s předchozím souhlasem původce informace.
TLP: AMBER	Informaci je možné sdílet pouze s omezeným okruhem osob (určuje původce); příjemci mohou sdílet tyto informace pouze s členy své organizace a s dodavateli nebo zákazníky, kteří nezbytně potřebují tyto informace znát, aby se chránili nebo zabránili vzniku další škody; původce informace může rozsah sdílení dále omezit.
TLP: GREEN	Informace je určena k omezenému zveřejnění; omezeno na komunitu (organizace příjemce a další partnerské subjekty příjemce informace), avšak nikoliv s využitím veřejně dostupných komunikačních kanálů; příjemce nesmí informaci šířit mimo určenou komunitu (určuje původce).
TLP: WHITE	Zveřejnění informace není omezeno; tímto ustanovením není dotčeno omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran.

Přehled poskytnutých prací – nutno doplnit

ID	Činnosti	Odborná role	Počet člověkohodin	Datum
1	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
2	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
3	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
4	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
5	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
6	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
7	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
8	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
9	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
10	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
	Součet		nutno doplnit	

Příloha č. x

Přehled poskytnutých prací – nutno doplnit

ID	Činnosti	Odborná role	Počet člověkohodin	Datum
1	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
2	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
3	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
4	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
5	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
6	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
7	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
8	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
9	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
10	nutno doplnit	nutno doplnit	nutno doplnit	nutno doplnit
	Součet		nutno doplnit	

Vykazované období:	**od DD.MM.RRRR do DD.MM.RRRR**

Prováděcí smlouva	**Cena v Kč bez DPH**	**DPH v Kč**	**Cena v Kč včetně DPH**
Služby poskytování infrastruktury – APAO	nutno doplnit	nutno doplnit	nutno doplnit
Služby poskytování infrastruktury – AISG	nutno doplnit	nutno doplnit	nutno doplnit
Služby poskytování infrastruktury – EESS	nutno doplnit	nutno doplnit	nutno doplnit
Služby datového centra	nutno doplnit	nutno doplnit	nutno doplnit
Provozní služby – APAO	nutno doplnit	nutno doplnit	nutno doplnit
Provozní služby – AISG	nutno doplnit	nutno doplnit	nutno doplnit
Provozní služby – AISG AM	nutno doplnit	nutno doplnit	nutno doplnit
Provozní služby – EESS	nutno doplnit	nutno doplnit	nutno doplnit
Poskytování odborných rolí	nutno doplnit	nutno doplnit	nutno doplnit
Celkem	**nutno doplnit**	**nutno doplnit**	**nutno doplnit**

Akceptace služeb	
Za Dodavatele	
Jméno, příjmení Oprávněné osoby Dodavatele: **nutno doplnit**	Podpis:
Za Objednatele	
Jméno, příjmení – věcná akceptace APAO a čerpání odborných rolí **nutno doplnit**	Podpis:

Jméno, příjmení – věcná akceptace AISG **nutno doplnit**	Podpis:
Jméno, příjmení – věcná akceptace EESS **nutno doplnit**	Podpis:
Jméno, příjmení – věcná akceptace Datové centrum **nutno doplnit**	Podpis:
Jméno, příjmení – věcná akceptace Datové centrum **nutno doplnit**	Podpis:
Jméno, příjmení Oprávněné osoby Objednatele: **nutno doplnit**	Podpis:

Štítek	Podmínky použití
TLP: RED	Informace není určena pro jiné než určené osoby (určuje původce); poskytnutí informace dalším subjektům ze strany příjemce lze učinit pouze s předchozím souhlasem původce informace.
TLP: AMBER	Informaci je možné sdílet pouze s omezeným okruhem osob (určuje původce); příjemci mohou sdílet tyto informace pouze s členy své organizace a s dodavateli nebo zákazníky, kteří nezbytně potřebují tyto informace znát, aby se chránili nebo zabránili vzniku další škody; původce informace může rozsah sdílení dále omezit.
TLP: GREEN	Informace je určena k omezenému zveřejnění; omezeno na komunitu (organizace příjemce a další partnerské subjekty příjemce informace), avšak nikoliv s využitím veřejně dostupných komunikačních kanálů; příjemce nesmí informaci šířit mimo určenou komunitu (určuje původce).

TLP: WHITE	Zveřejnění informace není omezeno; tímto ustanovením není dotčeno omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran.

ZÁZNAM O POSKYTNUTÍ SLUŽEB

dle Smlouvy BDC 2024+

Vykazované období:	od DD.MM.RRRR do DD.MM.RRRR

Obě Smluvní strany potvrzují, že v uvedeném období byly v souladu s výše uvedenou Smlouvou poskytnuty níže specifikované Služby v účtovaném množství:

KL	Cena v Kč bez DPH	DPH v Kč	Cena v Kč včetně DPH
Služby poskytování infrastruktury – APAO	nutno doplnit	nutno doplnit	nutno doplnit
Služby poskytování infrastruktury – AISG	nutno doplnit	nutno doplnit	nutno doplnit
Služby poskytování infrastruktury – EESS	nutno doplnit	nutno doplnit	nutno doplnit
Služby datového centra	nutno doplnit	nutno doplnit	nutno doplnit
Provozní služby – APAO	nutno doplnit	nutno doplnit	nutno doplnit
Provozní služby – AISG	nutno doplnit	nutno doplnit	nutno doplnit
Provozní služby – AISG AM	nutno doplnit	nutno doplnit	nutno doplnit
Provozní služby – EESS	nutno doplnit	nutno doplnit	nutno doplnit
Poskytování odborných rolí	nutno doplnit	nutno doplnit	nutno doplnit
Celkem	**nutno doplnit**	**nutno doplnit**	**nutno doplnit**

Detailní přehled příslušných Služeb poskytování infrastruktury a Provozních služeb pro jednotlivé informační systémy bude uveden v měsíční Zprávě o úrovni a rozsahu poskytovaných služeb.

Akceptace služeb	
Za Dodavatele	
Jméno, příjmení Oprávněné osoby Dodavatele: **nutno doplnit**	Podpis:
Za Objednatele	
Jméno, příjmení – věcná akceptace APAO a čerpání odborných rolí **nutno doplnit**	Podpis:
Jméno, příjmení – věcná akceptace AISG **nutno doplnit**	Podpis:
Jméno, příjmení – věcná akceptace EESS **nutno doplnit**	Podpis:
Jméno, příjmení – věcná akceptace Datové centrum **nutno doplnit**	Podpis:
Jméno, příjmení – věcná akceptace Datové centrum **nutno doplnit**	Podpis:
Jméno, příjmení Oprávněné osoby Objednatele: **nutno doplnit**	Podpis:

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.first.org/tlp/). Informace je označena příznakem, který stanoví

podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Podmínky využití poskytnutých informací

Štítek	Podmínky použití
TLP: RED	Informace není určena pro jiné než určené osoby (určuje původce); poskytnutí informace dalším subjektům ze strany příjemce lze učinit pouze s předchozím souhlasem původce informace.
TLP: AMBER	Informaci je možné sdílet pouze s omezeným okruhem osob (určuje původce); příjemci mohou sdílet tyto informace pouze s členy své organizace a s dodavateli nebo zákazníky, kteří nezbytně potřebují tyto informace znát, aby se chránili nebo zabránili vzniku další škody; původce informace může rozsah sdílení dále omezit.
TLP: GREEN	Informace je určena k omezenému zveřejnění; omezeno na komunitu (organizace příjemce a další partnerské subjekty příjemce informace), avšak nikoliv s využitím veřejně dostupných komunikačních kanálů; příjemce nesmí informaci šířit mimo určenou komunitu (určuje původce).
TLP: WHITE	Zveřejnění informace není omezeno; tímto ustanovením není dotčeno omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran.

ZÁZNAM O POSKYTNUTÍ SLUŽEB

dle Smlouvy BDC 2024+

Vykazované období:	od DD.MM.RRRR do DD.MM.RRRR

Obě Smluvní strany potvrzují, že v uvedeném období byly v souladu s výše uvedenou Smlouvou poskytnuty níže specifikované Služby v účtovaném množství:

KL	Cena v Kč bez DPH	DPH v Kč	Cena v Kč včetně DPH
Služby poskytování infrastruktury – ARES PRODUKCE	nutno doplnit	nutno doplnit	nutno doplnit
Služby poskytování infrastruktury – ARES TEST	nutno doplnit	nutno doplnit	nutno doplnit
Služby poskytování infrastruktury – ARES VÝVOJ	nutno doplnit	nutno doplnit	nutno doplnit
Provozní služby – ARES PRODUKCE	nutno doplnit	nutno doplnit	nutno doplnit
Provozní služby – ARES TEST	nutno doplnit	nutno doplnit	nutno doplnit
Provozní služby – ARES VÝVOJ	nutno doplnit	nutno doplnit	nutno doplnit
Cloudová služba – ARES PRODUKCE	nutno doplnit	nutno doplnit	nutno doplnit
Cloudová služba – ARES TEST	nutno doplnit	nutno doplnit	nutno doplnit
Cloudová služba – ARES VÝVOJ	nutno doplnit	nutno doplnit	nutno doplnit
Celkem	**nutno doplnit**	**nutno doplnit**	**nutno doplnit**

Detailní přehled Jednotek příslušných Služeb poskytování infrastruktury a Provozních služeb pro jednotlivé informační systémy bude uveden v měsíční Zprávě o úrovni a rozsahu poskytovaných služeb.

Akceptace služeb	
Za Dodavatele	
Jméno, příjmení Oprávněné osoby Dodavatele: **nutno doplnit**	Podpis:
Za Objednatele	
Jméno, příjmení – věcná akceptace ARES **nutno doplnit**	Podpis:
Jméno, příjmení Oprávněné osoby Objednatele: **nutno doplnit**	Podpis:

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.first.org/tlp/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Podmínky využití poskytnutých informací

Štítek	Podmínky použití
TLP: RED	Informace není určena pro jiné než určené osoby (určuje původce); poskytnutí informace dalším subjektům ze strany příjemce lze učinit pouze s předchozím souhlasem původce informace.
TLP: AMBER	Informaci je možné sdílet pouze s omezeným okruhem osob (určuje původce); příjemci mohou sdílet tyto informace pouze s členy své organizace a s dodavateli nebo zákazníky, kteří nezbytně potřebují tyto informace znát, aby se chránili nebo zabránili vzniku další škody; původce informace může rozsah sdílení dále omezit.
TLP: GREEN	Informace je určena k omezenému zveřejnění; omezeno na komunitu (organizace příjemce a další partnerské subjekty příjemce informace), avšak nikoliv s využitím veřejně dostupných komunikačních kanálů; příjemce nesmí informaci šířit mimo určenou komunitu (určuje původce).

TLP: WHITE	Zveřejnění informace není omezeno; tímto ustanovením není dotčeno omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran.

Vyhodnocení / akceptační protokol o odstranění kybernetické bezpečnostní události kybernetického bezpečnostního incidentu

Označení kybernetické bezpečnostní události/ kybernetického bezpečnostního incidentu	**KBI – 2021 – 0x**
Typ nahlášené KBU/KBI	kybernetická bezpečnostní událost kybernetický bezpečnostní incident
Významnost KBI	Kategorie I – méně významný kybernetický bezpečnostní incident Kategorie II – významný kybernetický bezpečnostní incident Kategorie III – velmi významný kybernetický bezpečnostní incident
KBI podle dopadu na aktiva	kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv kybernetický bezpečnostní incident způsobující narušení integrity aktiv kybernetický bezpečnostní incident způsobující narušení dostupnosti aktiv kybernetický bezpečnostní incident způsobující kombinaci dopadů uvedených shora
Vliv KBI na poskytované služby Ministerstva financí	Nedostupnost u služeb**:** IS KII: VIS: Ostatni IS: provozní IS Nedostupnost služby pro MF**:** IS KII: VIS: Ostatní IS:
Záměr KBI	Úmyslný / Neúmyslný
Začátek KBI:	17. 10. 2020 v 00:00
Konec KBI:	17. 10. 2020 v 00:00
Popis incidentu:	

Příčina incidentu:	
Incident vznikl jako následek	
Provedená okamžitá opatření:	
Organizační opatření: ***Technická opatření:***	
Činnost správce, provozovatele, operátora a uživatelů IS v průběhu incidentu:	
Na základě vyhodnocení bezpečnostního incidentu je nutné bez zbytečného odkladu provést:	
Opatření plánované pro předejití / zmírnění rizika opakování incidentu:	
Opatření organizační: ***Opatření technická:***	
Náklady bezpečnostního incidentu:	
Navrhované pořízení zařízení nebo služeb pro předejití / zmírnění rizika opakování incidentu	
Služby: ***Investice:***	
Vyhodnotil (jméno, příjmení): Datum: Podpis:	
Seznámení dotčených osob s vyhodnocením KBI a přijatými opatřeními Ministerstvo financí	
Manažer kybernetické bezpečnosti Ministerstva financí (jméno, příjmení): Akceptuji / neakceptuji Datum: Podpis:	