Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

RÁMCOVÁ SMLOUVA O POSKYTOVÁNÍ CLOUDOVÝCH A DALŠÍCH SOUVISEJÍCÍCH SLUŽEB

evidovaná u Objednatele pod č. VZ/2025/054/1317
evidovaná u Poskytovatele pod č. SML2025033, č. j. SPCSS-02205/2025
(dále jen „**Rámcová smlouva**")

Smluvní strany:

Objednatel: Česká republika – Ministerstvo pro místní rozvoj
se sídlem Staroměstské nám. 932/6, 110 00, Praha 1
zastoupený/á: [redacted]
IČO: 660 02 222
DIČ: není plátce DPH
ID datové schránky: 26iaava
bankovní spojení: [redacted]
číslo účtu: [redacted]

(dále jen „**Objednatel**")

a

Poskytovatel: 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: [redacted]
IČO: 03630919
DIČ: CZ03630919
ID datové schránky: ag5uunk
bankovní spojení: [redacted]
číslo účtu: [redacted]

(dále jen „**Poskytovatel**")

(Objednatel a Poskytovatel jednotlivě dále také jen **„Smluvní strana"** nebo společně také dále jen „**Smluvní strany**")

uzavřely níže uvedeného dne, měsíce a roku tuto Rámcovou smlouvu 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 „**Občanský zákoník**"), a příslušnými ustanoveními zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**").

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

I. ÚVODNÍ USTANOVENÍ

1.1 Objednatel prohlašuje, že:

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

1.1.2 ke dni uzavření této Rámcové smlouvy naplňuje podmínky pro využití vertikální spolupráce dle § 11 odst. 1 ZZVZ ve smyslu ZZVZ; Objednatel v této souvislosti prohlašuje, že bude i nadále dlouhodobě vyvíjet svou činnost tak, aby byly permanentně splněny tyto podmínky vertikální spolupráce dle současných právních předpisů a bude-li to možné, i podle právních předpisů budoucích po celou dobu trvání této Rámcové smlouvy, dojde-li v průběhu trvání této Rámcové smlouvy ke změně relevantní právní úpravy;

1.1.3 splňuje veškeré podmínky a požadavky v této Rámcové smlouvě stanovené a je oprávněn tuto Rámcovou smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.2 Poskytovatel prohlašuje, že:

1.2.1 je státním podnikem řádně zřízeným a existujícím podle zákona č. 77/1997 Sb., o státním podniku, ve znění pozdějších předpisů;

1.2.2 byl dne 20. 12. 2023 jmenován dle ust. §6i odst. 1 písm. a) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, poskytovatelem cloud computingu orgánům veřejné správy;

1.2.3 splňuje veškeré podmínky a požadavky v této Rámcové smlouvě stanovené a je oprávněn tuto Rácovou smlouvu uzavřít a řádně plnit závazky v ní obsažené;

1.2.4 ke dni uzavření této Rámcové smlouvy vůči němu není vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů, a zároveň se zavazuje Objednatele o všech skutečnostech o hrozícím úpadku bezodkladně informovat;

1.2.5 ke dni uzavření této Rámcové smlouvy naplňuje podmínky pro využití vertikální spolupráce dle § 11 odst. 1 ZZVZ ve smyslu ZZVZ; Poskytovatel v této souvislosti prohlašuje, že bude i nadále dlouhodobě vyvíjet svou činnost tak, aby byly permanentně splněny tyto podmínky vertikální spolupráce dle současných právních předpisů a bude-li to možné, i podle právních předpisů budoucích po celou dobu trvání této Rámcové smlouvy, dojde-li v průběhu trvání této Rámcové smlouvy ke změně relevantní právní úpravy;

1.2.6 v souladu s varováním Národního úřadu pro kybernetickou a informační bezpečnost vydaným podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, ze dne 21. 3. 2022, sp. zn. 350-401/2022, č. j. 3381/2022-NÚKIB-E/350 (dále jen „**Varování NÚKIB**"), nemá významný vztah k Ruské federaci, tj.:

1.2.6.1 nemá sídlo v Ruské federaci;

1.2.6.2 není závislý na dodávkách z území Ruské federace;

1.2.6.3 plnění dle Rámcové smlouvy nebude dodáváno prostřednictvím pobočky Poskytovatele v Ruské federaci;

1.2.6.4 plnění dle Rámcové smlouvy nemá svůj vývoj či výrobu lokalizovanou v Ruské federaci;

1.2.6.5 jeho významní Poskytovatelé ve smyslu § 2 písm. n) VoKB nepoužívají ICT služby či produkty závislé na Poskytovatelích s významným vztahem k Ruské federaci;

1.2.7 že na Poskytovatele ani jeho poddodavatele nedopadají mezinárodní sankce podle zákona č. 69/2006 Sb., o provádění mezinárodních sankcí (dále jen „**ZPMS**") (např. nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině), na základě kterých, Objednatel nesmí zpřístupnit finanční prostředky za plnění Rámcové smlouvy;

1.2.8 ve smyslu čl. 2 odst. 2 Nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny (dále jen „**Nařízení č. 269/2014**), není fyzickou nebo právnickou osobou, subjektem či orgánem nebo fyzickou nebo právnickou osobou, subjektem či orgánem s nimi spojeným uvedeným v příloze I Nařízení č. 269/2014. Pokud v průběhu účinnosti Rámcové smlouvy dojde k nedodržení podmínky dle věty první tohoto pododstavce, zavazuje se Poskytovatel bezodkladně o této skutečnosti písemně informovat Objednatele;

1.2.9 že ve smyslu varování Národního úřadu pro kybernetickou a informační bezpečnost, vydaného podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, ze dne 8. 3. 2023, sp. zn. 350–303/2023, č. j. 2236/2023-NÚKIB-E/350 (dále jen „**Varování II**") nemá nainstalován a nepoužívá aplikaci TikTok na zařízeních přistupujících k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům;

1.2.10 je oprávněn Rámcovou 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**");

1.2.11 si je vědom skutečnosti, že označování dokumentů vzniklých na základě této Rámcové smlouvy bude probíhat v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.first.org/tlp/). Dokumenty budou označeny příznakem, který stanoví podmínky použití informací v těchto dokumentech. Smluvní strany níže svým podpisem stvrzují, že v průběhu vyjednávání o této Rámcové smlouvě vždy jednaly čestně a transparentně a současně se zavazují, že takto budou jednat i při plnění této Rámcové smlouvy, a to po celou dobu její účinnosti.

1.3 Smluvní strany níže svým podpisem stvrzují, že v průběhu vyjednávání o této Rámcové smlouvě vždy jednaly čestně a transparentně a současně se zavazují, že takto budou jednat i při plnění této Rámcové smlouvy, a to po celou dobu její účinnosti;

1.4 Každá ze Smluvních stran prohlašuje:

1.4.1 že se nepodílí a ani v minulosti nepodílela na páchání trestné činnosti v jakékoli formě ve smyslu zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, v platném znění (dále jen „**ZTOPO**");

1.4.2 že zavedla potřebná opatření, aby nedošlo ke spáchání trestného činu v jakékoli formě, který by jí mohl být přičten podle ZTOPO;

1.4.3 že zavedla náležitá kontrolní a jiná obdobná opatření nad činností svých zaměstnanců, aby nevznikla trestní odpovědnost fyzických osob podle zákona č. 40/2009 Sb., trestní zákoník;

1.4.4 že učinila nezbytná opatření k zamezení nebo odvrácení případných následků spáchaného trestného činu a

1.4.5 že z hlediska prevence trestní odpovědnosti právnických osob učinila vše, co po ní lze spravedlivě požadovat, např. přijala Etický kodex a zásady Compliance programu.

1.5 Každá ze Smluvních stran prohlašuje, že nebude tolerovat jednání, které by mohlo naplňovat skutkové podstaty korupčních trestných činů, zejména trestných činů přijetí úplatku, nepřímého úplatkářství, podplácení a legalizace výnosů z trestné činnosti, přičemž důvodné podezření ohledně možného naplnění skutkové podstaty těchto trestných činů je příslušná Smluvní strana povinna neprodleně oznámit druhé Smluvní straně bez ohledu a nad rámec splnění případné zákonné oznamovací povinnosti.

1.6 V této souvislosti se Smluvní strany zavazují si navzájem neprodleně oznámit důvodné podezření ohledně možného jednání, které je v rozporu se zásadami podle odst. 1.3 až 1.7 tohoto článku a mohlo by souviset s plněním této Rámcové smlouvy nebo s jejím uzavíráním.

1.7 Smluvní strany prohlašují, že jsou jim známy zásady, hodnoty a cíle druhé Smluvní strany a zavazují se v co nejširším možném rozsahu (pokud to povaha jednotlivých ustanovení umožňuje) tyto zásady a hodnoty dodržovat, a to na vlastní náklady a odpovědnost při plnění svých závazků vzniklých z této Rámcové smlouvy.

1.8 Poskytovatel se zavazuje udržovat tato svá prohlášení dle odst. 1.2 až 1.7 v platnosti pro celou dobu účinnosti této Rámcové smlouvy.

II. ÚČEL RÁMCOVÉ SMLOUVY

2.1 Rámcová smlouva je uzavírána za účelem sjednání základních rámcových podmínek pro poskytování cloudových služeb Poskytovatele souvisejících se zajištěním infrastruktury a integračních vazeb, služeb kybernetické bezpečnosti a dalších služeb souvisejících s předmětnými cloudovými službami a službami kybernetické bezpečnosti pro informační systém eTurista. K dosažení tohoto cíle chce Objednatel využít Poskytovatelem poskytované plnění na základě jednotlivých objednávek.

III. PŘEDMĚT RÁMCOVÉ SMLOUVY

3.1 Předmětem této Rámcové smlouvy je úprava vzájemných práv a povinností Smluvních stran pro účely zajištění infrastruktury a integračních vazeb v cloudovém prostředí Poskytovatele, služeb kybernetické bezpečnosti a souvisejících služeb dle specifikace uvedené v odst. 3.3 tohoto článku, předmětem této Rámcové smlouvy je tak stanovení podmínek, za kterých bude docházet mezi Smluvními stranami k uzavírání objednávek (dále jen „**Objednávka**“) za podmínek dále specifikovaných v této Rámcové smlouvě.

3.2 Předmětem Rámcové smlouvy je mimo jiné také zakotvení oprávnění Objednatele vyzvat Poskytovatele v souladu s postupem uvedeným v čl. V a VI Rámcové smlouvy k uzavření Objednávek na služby specifikované v odst. 3.3 tohoto článku, a tyto Objednávky s ním následně za podmínek stanovených Rámcovou smlouvou uzavřít a dále zakotvení závazku Poskytovatele na základě výzvy Objednatele uzavřít za podmínek stanovených Rámcovou smlouvou Objednávku.

3.3 Předmětem plnění je závazek Poskytovatele na základě Objednávek poskytnout Objednateli cloudové služby SPCSS, resp. Poskytovatele a služby odborných činností, které zahrnují:

3.3.1 služby pro zajištění provozu cloudové platformy Poskytovatele zahrnující cloudové služby, tj. poskytování provozu služeb infrastruktury, konektivity a dalších souvisejících služeb (to vše dále jen **„Cloudové služby**“), a to dle nabídky služeb zveřejněné na webové adrese uvedené v Příloze č. 3 Rámcové smlouvy (jedná se pouze o služby poskytované Poskytovatelem Státní pokladna Centrum sdílených služeb, s. p., ID 71) (dále jen „**Katalog Cloudových služeb**“), a to vždy dle volby Objednatele**;**

3.3.2 služby kybernetické bezpečnosti, které zahrnují následující služby:

3.3.2.1 Bezpečnostní monitoring - zahrnuje sběr informací, jejich třídění, korelaci, kategorizaci, analýzu a archivaci a incident management;

3.3.2.2 Vurnerability management - skenování zranitelností probíhající jedenkrát měsíčně nebo manuálním Ad-hoc skenem (např. při zveřejnění kritické zranitelnosti);

3.3.2.3 Kompetenční Centrum Kybernetické Bezpečnosti (KCKB) - zahrnuje podporu činností vyplývajících pro povinné osoby z právních předpisů (zejména zákon č. 181/2014 Sb., o kybernetické bezpečnosti, resp. vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti);

3.3.2.4 Správa privilegovaných účtů - správa přístupu k privilegovaným účtům a monitoring veškeré aktivity účtů s vazbou na konkrétní osobu, která jím právě disponuje;

(vše v pododst. 3.3.2 dále jen „**Služby KB**"), přičemž podrobný popis Služeb KB je uveden v jednotlivých katalogových listech v Příloze č. 4 Smlouvy. Smluvní strany berou na vědomí a souhlasí s tím, že poskytování jednotlivých Služeb KB musí a bude vždy předcházet Objednávka na Proof Of Concept (dále jen „**PoC**" nebo „**Realizace ověření provozu**"), přičemž pro poskytování PoC se analogicky uplatní stejné podmínky jako pro Služby KB, vyjma dodržování závazných SLA, není-li dále v Rámcové smlouvě výslovně uvedeno jinak.

3.3.3 služby odborných činností zahrnující:

3.3.3.1 ostatní činnosti související s Cloudovými službami a Službami KB, poskytované prostřednictvím odborných rolí uvedených v Příloze č. 1 Rámcové smlouvy (dále jen „**Ostatní činnosti**"), přičemž se jedná zejména o následující činnosti, tj.:

a) analýzu stavu Cloudových služeb nebo Služeb KB a návrh rozšíření nebo změny;

b) implementaci schváleného řešení;

c) školení pracovníků Objednatele a dalších osob dle zadání Objednatele;

d) aktualizaci nebo tvorbu dokumentace ke Cloudovým službám a Službám KB;

e) přípravu Cloudových služeb, popř. Služeb KB dle specifikace dodané Objednatelem;

3.3.3.2 konzultační, poradenské a další činnosti na vyžádání, které nejsou Ostatními činnostmi, v oblasti Cloudových služeb a Služeb KB, poskytované prostřednictvím odborných rolí uvedených v Příloze č. 1 Rámcové smlouvy (dále jen „**Konzultace**")

(vše v pododst. 3.3.3 dále jen „**Odborné činnosti**").

(Cloudové služby a Odborné činnosti a Služby KB dále společně také jen „**Služby**" nebo samostatně jen „**Služba**").

3.4 Předmětem této Rámcové smlouvy je zároveň závazek Objednatele za řádně poskytnuté Služby uhradit Poskytovateli cenu dle čl. VIII této Rámcové smlouvy.

3.5 Objednatel se zavazuje poskytnout Poskytovateli veškerou součinnost, nezbytnou pro řádné splnění Rámcové smlouvy ze strany Poskytovatele.

3.6 Poskytovatel prohlašuje, že disponuje veškerými potřebnými oprávněními pro poskytnutí Služeb.

3.7 Poskytovatel je při uzavírání, jakož i při plnění Objednávek povinen postupovat v souladu s touto Rámcovou smlouvou a danou Objednávkou. Smluvní strany výslovně uvádějí a souhlasí s tím, že podmínkou uzavření Objednávek na Cloudové služby může být nutné uzavření Objednávky na Ostatní činnosti, zahrnující přípravu dané Cloudové služby (např. pokud dochází k spuštění/zahájení požadované Cloudové služby). Poskytovatel bude o této skutečnosti vždy Objednatele informovat a Objednatel bere tuto skutečnost na vědomí a souhlasí s tím, že bez uzavření předmětné Objednávky na Ostatní činnosti nelze požadovat uzavření Objednávky na Cloudové služby.

3.8 Pro vyloučení pochybností Smluvní strany uvádějí že v případě rozporu Rámcové smlouvy a Objednávek, popř. jejich příloh, mají vždy přednost ustanovení Rámcové smlouvy.

IV. DOBA, MÍSTO A ZPŮSOB PLNĚNÍ

4.1 Smluvní strany sjednávají, že doba plnění příslušné Služby bude vždy stanovena v příslušné Objednávce uzavřené dle této Rámcové smlouvy. Pro vyloučení pochybností Smluvní strany výslovně sjednávají, že účinnost každé Objednávky nastane nejdříve zveřejněním Objednávky v registru smluv v souladu se Zákonem o registru smluv.

4.2 Místem plnění jsou datová centra Poskytovatele na adresách: Na Vápence 915/14, Žižkov, 130 00 Praha 3 (dále jen „**DCV**") a Čsl. Armády 1060, 250 91 Zeleneč (dále jen „**DCZ**"), nedohodnou-li se Smluvní strany v rámci příslušné Objednávky jinak.

4.3 Plnění může být poskytnuto i vzdáleným přístupem, pokud to povaha plnění dle Rámcové smlouvy umožňuje, není-li nezbytné nebo vhodné výkon takového plnění zajistit on-site.

4.4 Poskytovatel se zavazuje poskytovat Cloudové služby a Služby KB v kvalitě definované vždy v dané Objednávce, resp. v daném Katalogovém listu v případě Služeb KB.

V. ZPŮSOB PLNĚNÍ – CLOUDOVÉ SLUŽBY A SLUŽBY KB

5.1 Poskytovatel se zavazuje poskytovat Cloudové služby a Služby KB ve vyžádaném rozsahu a kvalitě. Předmětné Služby budou Poskytovatelem poskytovány na základě písemné výzvy, zaslané Objednatelem Poskytovateli (dále jen „**Výzva**"). Výzva musí zejména obsahovat:

5.1.1 konkrétní označení a bližší specifikaci předmětných Cloudových služeb, resp. Služeb KB, které jsou poptávány s odkazem na Katalog Cloudových služeb, který je uveden v Příloze č. 3, popř. na konkrétní Katalogový list dle Přílohy č. 4 v případě Služeb KB;

5.1.2 požadovanou dobu poskytování předmětných Cloudových služeb, resp. Služeb KB;

5.1.3 Objednatelem předpokládaný rozsah daných Cloudových služeb, resp. Služeb KB.

5.2 Poskytovatel se zavazuje v souladu s Výzvou zpracovat nabídku dle příslušného vzoru uvedeného v Příloze č. 2 Rámcové smlouvy (dále jen „**Nabídka**") na poskytnutí poptávaných Cloudových služeb dle Katalogu Cloudových služeb, resp. dle Přílohy č. 4 Rámcové smlouvy v případě Služeb KB. Pro vyloučení pochybností Smluvní strany uvádějí, že pokud Poskytovatel neurčí jinak, je předpokladem zpracování Nabídky na dané Cloudové služby zpracování dokumentu High Level Design a předpokladem zpracování Nabídky na Služby KB zpracování dokumentu Vstupní analýzy, a to vždy na základě samostatné Objednávky na Ostatní činnosti. A současně v případě, že k poskytování některé z předmětných Cloudových služeb, resp. Služeb KB je nutná příprava dané Cloudové služby, resp. Služby KB ze strany Poskytovatele, je nezbytné rovněž vždy uzavřít samostatnou Objednávku na Ostatní činnosti zahrnující přípravu dané Cloudové služby, resp. Služby KB. Tj. bez uvedených kroků (přípravy příslušného dokumentu, popř. samotné přípravy dané Cloudové služby, resp. Služby KB a následné Objednávky na PoC v případě Služeb KB) nelze uzavřít následnou Objednávku na poskytování kterékoliv z daných Cloudových služeb, resp. Služeb KB. Na základě zpracovaného dokumentu, tj. High Level Design nebo Vstupní analýzy, vypracuje Poskytovatel Nabídku na danou Cloudovou službu/služby, resp. Službu KB, přičemž tato Nabídka musí obsahovat zejména následující náležitosti:

5.2.1 identifikační údaje Objednatele a Poskytovatele;

5.2.2 termín zahájení a ukončení poskytování předmětné Cloudové služby, resp. služeb nebo Služeb KB;

5.2.3 podrobnou specifikaci požadovaných Cloudových služeb, vč. technické přílohy (katalogového listu/listů) nebo Služeb KB;

5.2.4 cenu za danou Cloudovou službu/ Cloudové služby nebo Služby KB;

5.2.5 smluvní sankce (pokud jsou účelné);

5.2.6 případné požadavky na součinnosti Objednatele;

5.2.7 kvalifikovaný elektronický podpis Poskytovatele.

5.3 Poskytovatel zašle Nabídku Objednateli, a to ve lhůtě 15 pracovních dnů ode dne doručení Výzvy v případě, že k danému zpracování Nabídky není nutný High Level Design, resp. Vstupní analýza, popř. ve lhůtě 20 pracovních dnů ode dne podpisu Akceptačního protokolu bez výhrad v rámci dané Objednávky na Ostatní činnosti (tj. ode dne akceptace předmětného High Level Design, resp. Vstupní analýzy bez výhrad), přičemž. Poskytovatel se zavazuje, že Nabídka bude reflektovat Výzvou požadovaný rozsah dané Cloudové služby, resp. Cloudových služeb nebo Služeb KB. V případě, že Výzva nebude odpovídat náležitostem dle odst. 5.1 tohoto článku, je Poskytovatel oprávněn Výzvu Objednateli vrátit k doplnění, resp. opravě. V případě doručení doplněné/opravené Výzvy bude postupováno analogicky dle odst. 5.2 a násl. tohoto článku.

5.4 Objednatel se zavazuje nejpozději ve lhůtě 10 pracovních dnů ode dne doručení Nabídky posoudit soulad Nabídky s Výzvou a ve stejné lhůtě Nabídku buď akceptovat formou Objednávky (která bude reflektovat veškeré náležitosti stanovené Nabídkou), jejíž vzor je uveden v Příloze č. 2 Rámcové smlouvy, podepsat a zaslat Poskytovateli, případně ve stejné lhůtě požádat o změnu nebo upřesnění Nabídky nebo Nabídku odmítnout.

5.5 Poskytovatel se zavazuje doručenou Objednávku (zpracovanou v souladu s Nabídkou) podepsat a zaslat ve lhůtě 5 pracovních dnů ode dne doručení Objednávky zpět Objednateli, nedohodnou-li se Smluvní strany písemně na delší lhůtě. Okamžikem doručení podepsané Objednávky Objednateli dochází k uzavření závazné Objednávky. Pro vyloučení pochybností Smluvní strany uvádějí, že účinnost dané Objednávky nastane nejdříve zveřejněním Objednávky v registru smluv v souladu se Zákonem o registru smluv, přičemž Poskytovatel se zavazuje Objednávku vždy zveřejnit v Registru smluv a o této skutečností bezodkladně informovat Objednatele.

5.6 V případě, že si Objednatel vyžádá úpravu Nabídky, je Poskytovatel povinen tuto úpravu provést bez zbytečného odkladu za obdobného použití odst. 5.2 této Rámcové smlouvy.

5.7 Poskytovatel se zavazuje poskytovat dané Cloudové služby a Služby KB v souladu s Objednávkou, tj. způsobem a v termínech uvedených v Objednávce.

VI. AKCEPTACE PLNĚNÍ – CLOUDOVÉ SLUŽBY A SLUŽBY KB

6.1 Poskytnutí Cloudových služeb, resp. Služeb KB bude Objednatelem přebíráno na základě samostatných, popř. společných potvrzení o poskytnutí předmětných Cloudových služeb, resp. Služeb KB vždy za daný kalendářní měsíc poskytování daných Cloudových služeb, resp. Služeb KB dle předmětných Objednávek a bude realizováno formou podpisu samostatných, popř. společného záznamu o poskytnutí předmětných Cloudových služeb, resp. Služeb KB (dále jen „**Záznam**"), jehož vzor je součástí Přílohy č. 2 Rámcové smlouvy, přičemž Poskytovatel vystaví Záznam vždy do 5 pracovních dnů následujících po skončení kalendářního měsíce, ve kterém byly předmětné Cloudové služby, resp. Služby KB 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 předmětných Cloudových služeb, resp. Služeb KB budou řešeny v rámci Zprávy postupem dle odst. 6.2 tohoto článku.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

6.2 Hodnocení a kontrola poskytování předmětných Cloudových služeb, resp. Služeb KB v daném kalendářním měsíci bude probíhat vždy za daný kalendářní měsíc na základě zprávy o úrovni a rozsahu poskytovaných služeb (dále jen „**Zpráva**"), jejíž vzor je součástí Přílohy č. 2 Rámcové smlouvy, kterou vyhotoví Poskytovatel a předloží ji Oprávněné osobě Objednatele ve lhůtě 10 pracovních dnů ode dne skončení příslušného kalendářního měsíce, ve kterém byly předmětné Cloudové služby, resp. Služby KB poskytovány. 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 předmětných Cloudových služeb, resp. Služeb KB 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 Rámcovou smlouvou, tj. při nedodržení stanovených podmínek pro poskytování předmětných Cloudových služeb, resp. Služeb KB, popř. některé z nich, je Objednatel oprávněn uplatnit příslušné sankce dle Rámcové smlouvy, resp. dané Objednávky.

6.3 Na základě vyhodnocení Zprávy v příslušném období mohou Oprávněné osoby Smluvních stran navrhnout přijetí případných změn v poskytování předmětných Cloudových služeb, resp. Služeb KB, vč. cenových dopadů, a to formou změnového řízení postupem dle čl. IX Rámcové smlouvy.

VII. ZPŮSOB A AKCEPTACE PLNĚNÍ – ODBORNÉ ČINNOSTI

7.1 Poskytovatel se zavazuje poskytovat Ostatní činnosti ve vyžádaném rozsahu a kvalitě. Ostatní činnosti budou Poskytovatelem poskytovány na základě Výzvy Objednatele k poskytnutí Ostatních činností. Výzva musí zejména obsahovat:

7.1.1 konkrétní označení a bližší specifikaci Ostatních činností, které jsou poptávány a zda má být plněno jako celek nebo po částech;

7.1.2 požadovaný termín dodání Ostatních činností;

7.1.3 Objednatelem předpokládaný rozsah Ostatních činností a cenu za Ostatní činnosti stanovenou v souladu s cenovými podmínkami uvedenými v této Rámcové smlouvě (zejména dle počtu objednaných člověkodnů pro danou roli).

7.2 Poskytovatel se zavazuje v souladu s Výzvou zpracovat Nabídku na poskytnutí Ostatních činností a odeslat Nabídku Objednateli do 15 pracovních dnů od doručení Výzvy Poskytovateli, nedohodnou-li se Smluvní strany písemně na delší lhůtě. Poskytovatel se zavazuje, že Nabídka bude reflektovat Výzvou požadovaný rozsah Ostatních činností. Pokud Poskytovatel sdělí Objednateli vady ve vymezení Výzvy bránící Poskytovateli Nabídku vypracovat, Objednatel je povinen Poskytovatelem specifikované vady Výzvy odstranit a Výzvu opětovně předložit.

7.3 Objednatel se zavazuje nejpozději ve lhůtě 10 pracovních dnů ode dne doručení Nabídky posoudit soulad Nabídky s Výzvou a ve stejné lhůtě Nabídku buď akceptovat formou Objednávky, jejíž vzor je uveden v Příloze č. 2 Rámcové smlouvy, podepsat a zaslat Poskytovateli, případně ve stejné lhůtě požádat o změnu nebo upřesnění Nabídky nebo Nabídku odmítnout.

7.4 Poskytovatel se zavazuje doručenou Objednávku (zpracovanou v souladu s Nabídkou) podepsat a zaslat ve lhůtě 5 pracovních dnů ode dne doručení Objednávky zpět Objednatel, nedohodnou-li se Smluvní strany písemně na delší lhůtě. Okamžikem doručení podepsané Objednávky Objednateli dochází k uzavření závazné Objednávky. Pro vyloučení pochybností Smluvní strany uvádějí, že účinnost dané Objednávky nastane nejdříve zveřejněním Objednávky v registru smluv v souladu se Zákonem o registru smluv, přičemž Poskytovatel se zavazuje Objednávku vždy zveřejnit v Registru smluv a o této skutečnosti bezodkladně informuje Objednatele.

7.5 V případě, že si Objednatel vyžádá úpravu Nabídky, je Poskytovatel povinen tuto úpravu provést bez zbytečného odkladu za obdobného použití odst. 7.2 této Rámcové smlouvy.

7.6 Poskytovatel se zavazuje poskytovat Ostatní činnosti v souladu s Objednávkou, tj. způsobem a v termínech uvedených v Objednávce.

7.7 Hodnocení, kontrola plnění a akceptace Ostatních činností bude probíhat vždy za každé jednotlivé plnění, resp. za každou jednotlivou Objednávku následujícím způsobem:

7.7.1 hodnocení, kontrolu plnění a akceptaci Ostatních činností provádějí Oprávněné osoby Smluvních stran;

7.7.2 akceptaci plnění Ostatních činností na základě příslušné Objednávky bude provádět Oprávněná osoba Objednatele na základě příslušného akceptačního protokolu, jehož vzor je uveden v Příloze č. 2 Rámcové smlouvy (dále jen „**Akceptační protokol**"), který bude vystaven k celému plnění nebo k jednotlivým dílčím částem, pokud byly v Objednávce specifikovány.

7.7.3 Oprávněná osoba Poskytovatele se zavazuje předložit Oprávněné osobě Objednatele prostřednictvím e-mailu ke schválení Akceptační protokol vždy v termínu stanoveném v Objednávce pro dodání Ostatních činností, tj. spolu s předáním výstupu Ostatních činností (v případě Akceptačního protokolu vyhotoveného v elektronické podobě s elektronickými podpisem Oprávněné osoby Poskytovatele v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů);

7.7.4 Oprávněná osoba Objednatele se zavazuje ve lhůtě 5 pracovních dnů ode dne doručení Akceptačního protokolu poskytnuté Ostatní činnosti převzít a schválit Akceptační protokol svým podpisem (v případě Akceptačního protokolu vyhotoveného v elektronické podobě s elektronickým podpisem v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů), příp. uvést v Akceptačním protokolu výhrady k poskytnutým Ostatním činnostem, popř. Ostatní činnosti odmítnout (v případě, že výstupy neobsahují podstatné části, nebo obsahují vážné nedostatky, které znemožňují plnohodnotné užívání výstupu nebo způsobují vážné provozní problémy, a nelze je převzít s výhradami, kdy v takovém případě, tj. v případě odmítnutí převzetí, nemá opětovné předložení Ostatních činností Poskytovatelem k akceptaci vliv na termín plnění stanovený v Objednávce). Poskytovatel se zavazuje odstranit případné výhrady ve lhůtě 10 pracovních dnů ode dne doručení výhrad, nedohodnou-li se Smluvní strany písemně na kratší, popřípadě delší lhůtě. Po odstranění veškerých výhrad sepíšou Smluvní strany nový Akceptační protokol bez výhrad. Kopie Akceptačního protokolu bez výhrad bude vždy přílohou příslušné faktury za poskytnutí Ostatních činností.

7.8 Realizace Konzultací bude probíhat na základě jednotlivých Objednávek uzavíraných vždy do vyčerpání objednaného počtu člověkohodin uvedeného v Objednávce nebo do termínu stanoveného v Objednávce, podle toho, která ze skutečností nastane dříve. Přičemž účinnost Objednávky nastane nejdříve zveřejněním Objednávky v registru smluv v souladu se Zákonem o registru smluv, přičemž Poskytovatel se zavazuje Objednávku vždy zveřejnit v Registru smluv a o této skutečnosti bezodkladně informuje Objednatele. Objednávky budou uzavírány na základě písemné objednávky Objednatele na poskytnutí Konzultací, zaslané Oprávněné osobě Poskytovatele, která je návrhem na uzavření Objednávky, a písemným potvrzením přijetí návrhu Objednávky, tj. podpisem návrhu Objednávky ze strany Poskytovatele a jeho doručením Oprávněné osobě Objednatele, přičemž vzor Objednávky je součástí Přílohy č. 2 Rámcové smlouvy. Návrh Objednávky musí obsahovat zejména tyto náležitosti:

7.8.1 identifikační údaje Objednatele a Poskytovatele;

7.8.2 požadovaný termín provedení Konzultací, resp. doby trvání Objednávky a Místo plnění;

7.8.3 rozsah Konzultací, tj. uvedení počtu objednaných člověkohodin pro jednotlivé role dle Přílohy č. 1 Rámcové smlouvy;

7.8.4 maximální cenu za Konzultace stanovenou v souladu s cenovými podmínkami uvedenými v této Rámcové smlouvě (dle počtu objednaných člověkohodin pro jednotlivé role);

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

7.8.5 příp. další volitelné parametry v souladu s Rámcovou smlouvou;

7.8.6 podpis Objednatele.

7.8.7 podrobnou specifikaci požadovaných Konzultací, zejm. uvedení požadovaných oblastí, pro které mají být Konzultace poskytovány.

7.9 Poskytovatel se zavazuje provést potvrzení návrhu Objednávky ve lhůtě 5 pracovních dnů ode dne doručení návrhu Objednávky, nedohodnou-li se Smluvní strany prokazatelně písemně na delší lhůtě, popř. ve stejné lhůtě požádat Objednatele o doplnění či upřesnění chybějících náležitostí dle odst. 7.8 tohoto článku. Potvrzením návrhu Objednávky Poskytovatel vyjadřuje souhlas s obsahem Objednávky, a že nepožaduje doplnění či upřesnění chybějících náležitostí a jako takovou ji akceptuje. Požádá-li Poskytovatel o doplnění či upřesnění chybějících náležitostí, staví se lhůta pro potvrzení návrhu Objednávky do okamžiku zaslání řádně doplněného nového návrhu Objednávky. Poskytovatel není oprávněn návrh Objednávky jakýmkoliv způsobem doplňovat či měnit a zavazuje se návrh Objednávky potvrdit bez výhrad nebo požádat o doplnění či upřesnění podle tohoto odstavce. Potvrzení návrhu Objednávky s výhradou se nepovažuje za potvrzení návrhu Objednávky ve smyslu tohoto odstavce, není-li ve Rámcové smlouvě stanoveno jinak.

7.10 Při plnění Objednávek je Poskytovatel povinen postupovat v souladu s touto Rámcovou smlouvou a s danou Objednávkou. Na základě uzavřené Objednávky se Poskytovatel zavazuje poskytovat požadované Konzultace.

7.11 Objednatel může uzavírat s Poskytovatelem Objednávky podle svých potřeb po celou dobu účinnosti Rámcové smlouvy, a to postupem a za podmínek stanovených tímto článkem.

7.12 Poskytovatel se zavazuje poskytovat Konzultace v souladu s Objednávkou, tj. způsobem a v termínech uvedených v Objednávce.

7.13 Poskytovatel se zavazuje v rámci realizace Konzultací dle každé Objednávky vést výkaz Konzultací, v rámci, kterého prokazuje skutečně vynaložený čas na Konzultace pro jednotlivé role v člověkohodinách s přesností na dvě desetinná místa, a to vždy s uvedením konkrétních vykonaných činností v rámci Konzultací pro jednotlivé role (dále jen „**Výkaz Konzultací**"). Vzor Výkazu Konzultací je součástí Přílohy č. 2 Rámcové smlouvy.

7.14 Hodnocení, kontrola plnění a akceptace Konzultací bude probíhat vždy za každý uplynulý kalendářní měsíc účinnosti předmětné Objednávky, ve kterém byly Konzultace poskytovány.

7.15 Hodnocení, kontrolu plnění a akceptaci Konzultací provádějí Oprávněné osoby Smluvních stran, přičemž akceptaci plnění Konzultací na základě Výkazu Konzultací předloženého k akceptaci Poskytovatelem bude provádět Oprávněná osoba Objednatele.

7.16 Oprávněná osoba Poskytovatele se zavazuje předložit Oprávněné osobě Objednatele prostřednictvím e-mailu ke schválení Výkaz Konzultací za daný kalendářní měsíc, vždy do 5. pracovního dne kalendářního měsíce následujícího po kalendářním měsíci, v rámci kterého byly Konzultace poskytovány (v případě Výkazu Konzultací vyhotoveného v elektronické podobě s elektronickými podpisem Oprávněné osoby Poskytovatele v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů).

7.17 Oprávněná osoba Objednatele se zavazuje Výkaz Konzultací neprodleně, nejpozději však do 5 pracovních dnů od jeho předložení svým podpisem schválit (v případě Výkazu Konzultací vyhotoveného v elektronické podobě s elektronickým podpisem v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů), případně do něj uvést výhrady. Poskytovatel se zavazuje vypořádat případné výhrady nejpozději do 5 pracovních dnů od doručení podepsaného Výkazu Konzultací Objednatelem a výsledek sdělit písemně prostřednictvím emailu Oprávněné osobě Objednatele. Po odstranění případných výhrad sepíší Smluvní strany nový Výkaz Konzultací bez výhrad. V případě, že bude Výkaz Konzultací vyhotoven v listinné podobě, bude vyhotoven ve 2 stejnopisech, přičemž jeden bude ponechán Objednateli.

VIII. CENA A PLATEBNÍ PODMÍNKY

8.1 Poskytovatel se zavazuje provádět Cloudové služby dle jednotlivých Objednávek uzavíraných dle této Rámcové smlouvy s Objednatelem za ceny stanovené v souladu s tímto odstavcem (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 a v souladu s mechanismem popsaným na webových stránkách Poskytovatele uvedených v Příloze č. 3 Rámcové smlouvy.

8.2 Poskytovatel se zavazuje provádět Služby KB dle jednotlivých Objednávek uzavíraných dle této Rámcové smlouvy s Objednatelem na základě jednotkových cen stanovených v Příloze č. 5 Rámcové smlouvy (přičemž cena za danou Službu KB je stanovena dle Vstupní analýzy jako měsíční paušální cena pro jednotlivé Služby KYBE za jeden kalendářní měsíc poskytování dané Služby KB dle principu uvedeného v jednotlivých Katalogových listech v Příloze č. 4 Rámcové smlouvy, je stanovena dohodou Smluvních stran a je stanovena na základě zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů (dále jen „**Cena za Služby KB**").

8.3 Cena za poskytování Ostatních činností je stanovena jako součin rozsahu poskytnutých Ostatních činností Poskytovatelem v rámci předmětné Objednávky (resp. dílčí části v rámci dané Objednávky) vyjádřeného v člověkodnech v rámci dané role dle Přílohy č. 1 Rámcové smlouvy a jednotkové ceny za člověkoden pro danou roli uvedené v Příloze č. 1; v případě poskytování Ostatních činností v rámci dané Objednávky více rolemi se ceny za Ostatní činnosti pro jednotlivé role vypočtené dle předcházející věty sčítají (to vše dále jen „**Cena za Ostatní činnosti**"). V případě neposkytování Ostatních činností danou rolí po celý člověkoden se cena za Ostatní činnosti pro danou roli poměrně krátí s přesností na dvě desetinná místa.

8.4 Cena za poskytování Konzultací je stanovena jako součin prokazatelně vynaložených člověkohodin na poskytování Konzultací v předmětném kalendářním měsíci na základě dané Objednávky v rámci dané role dle Přílohy č. 1 Rámcové smlouvy a jednotkové ceny za člověkohodinu pro danou roli uvedené v Příloze č. 1; v případě poskytování Konzultací v rámci daného kalendářního měsíce více rolemi se ceny za Konzultace pro jednotlivé role vypočtené dle předcházející věty sčítají (to vše dále jen „**Cena za Konzultace**"). Poskytovatel bere na vědomí a souhlasí s tím, že jednotlivé doby poskytnuté na Konzultace v rámci příslušného kalendářního měsíce se sčítají dle vykázaného a Objednatelem schváleného času stráveného na poskytování Konzultací, přičemž Poskytovatelem může být účtován čas pro jednotlivé role s přesností na dvě desetinná místa.

8.5 K výše uvedeným cenám bude vždy připočítána DPH dle sazby daně ke dni uskutečnění zdanitelného plnění.

8.6 Smluvní strany se dohodly, že celkový souhrn plnění dle této Rámcové smlouvy, resp. všech Objednávek nesmí přesáhnout částku ve výši 64.000.000 Kč bez DPH (dále jen „**Maximální souhrnná cena**").

8.7 Poskytovatel prohlašuje, že je plátcem DPH.

8.8 Výše uvedené ceny jsou sjednány dohodou Smluvních stran podle zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů, a jsou cenami maximálními a nepřekročitelnými (není-li v Rámcové smlouvě výslovně uvedeno jinak), které zahrnují veškeré náklady spojené s realizací Služeb (např. správní a místní poplatky, vedlejší náklady, náklady spojené s dopravou do Místa plnění, včetně nákladů souvisejících s celními poplatky a s provedením všech zkoušek a testů prokazujících dodržení předepsané kvality a parametrů předmětu plnění dle Rámcové smlouvy apod.

8.9 Cena za Cloudové služby, resp. Cena za Služby KB bude uhrazena na základě faktury vystavené Poskytovatelem vždy zpětně za každý kalendářní měsíc poskytování Cloudových služeb, resp. Služeb KB, přičemž přílohou každé faktury bude vždy kopie potvrzeného Záznamu za příslušné období, přičemž dnem uskutečnění zdanitelného plnění je poslední den kalendářního měsíce, v němž byly předmětné Cloudové služby, resp. Služby KB poskytnuty.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

8.10 Cena za Ostatní činnosti bude Poskytovateli hrazena vždy po akceptaci poskytnutých Ostatních činností dle příslušné Objednávky, resp. dané dílčí části dle příslušné Objednávky, přičemž přílohou každé takové faktury musí být kopie příslušného Akceptačního protokolu bez výhrad.

8.11 Cena za Konzultace bude hrazena měsíčně, a to na základě Výkazu Konzultací podepsaného Objednatelem bez výhrad. Kopie Výkazu Konzultací bez výhrad bude tvořit přílohu faktury.

8.12 Poskytovatel doručí fakturu vždy elektronicky prostřednictvím datové schránky Objednatele.

8.13 Faktura musí obsahovat náležitosti obchodní listiny dle § 435 Občanského zákoníku 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:

8.13.1 přesnou specifikaci Služeb, za které je fakturováno;

8.13.2 číslo Rámcové smlouvy a Objednávky, číslo CES: **6754**;

8.13.3 specifikaci měsíce, za který se fakturuje, v případě, že se jedná o Cenu za Cloudové služby nebo Cenu za Služby KB;

8.13.4 v případě, že se jedná o Cenu za Konzultace uvedení člověkohodin a rolí, za které je fakturováno a v případě, že se jedná o Cenu za Ostatní činnosti rovněž uvedení člověkodnů a rolí, za které je fakturováno;

8.13.5 Cenu za Cloudové služby nebo Cenu za Ostatní činnosti nebo Cenu za Konzultace nebo Cenu za Služby KB;

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

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

8.15 Pokud nebude faktura obsahovat stanovené náležitosti nebo nebude obsahovat stanovené přílohy nebo v ní nebudou správně uvedené požadované údaje, je Objednatel oprávněn vrátit ji Poskytovateli před uplynutím lhůty splatnosti 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.

8.16 Veškeré platby dle této Rámcové smlouvy a Objednávek budou probíhat výhradně v korunách českých a rovněž veškeré cenové údaje dle této Rámcové smlouvy a Objednávek budou uvedeny v této měně.

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

8.18 Poskytovatel bere na vědomí, že Objednatel neposkytuje zálohy na poskytnutí Služeb.

8.19 Poskytovatel prohlašuje, že správce daně před uzavřením Rámcové 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.

8.20 Poskytovatel je oprávněn zvýšit každou z cen za Službu dle této Rámcové smlouvy s účinností od 1. dubna každého kalendářního roku následujícího po roce 2025 o přírůstek průměrného ročního indexu spotřebitelských cen (dále jen „**Míra inflace**") vyhlášeného Českým statistickým úřadem za předcházející kalendářní rok.

8.21 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.

8.22 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 tohoto článku není nutné uzavírat dodatek k Rámcové smlouvě.

8.23 Objednatel předpokládá, že část Služeb bude hrazena z rozpočtových položek přiřazených k projektu spolufinancovaného z Národního plánu obnovy (dále též „NPO"). Konkrétně se jedná o projekt „e-Turista-online registr ubytovaných hostů v ČR" (dále jen „**Projekt**"). Pro ty části Služeb bude Objednávky podepisovat spolu s Odpovědnou osobou pro věci smluvní Objednatele rovněž Oprávněná osoba Objednatele pro NPO. U nákladů, které bude Objednatel uplatňovat v rámci Projektu, bude na faktuře uveden název a registrační číslo Projektu následujícího znění: „název projektu: „e-Turista-online registr ubytovaných hostů v ČR", reg.č.: CZ.31.1.0/0.0/0.0/22_030/0008185". O skutečnosti, které Služby budou podléhat této povinnosti, bude Objednatel informovat Poskytovatele v rámci Výzvy a následně bude tato skutečnost uvedena rovněž do Objednávky.

8.24 Poskytovatel se zavazuje k plnění zásady významně nepoškozovat environmentální cíle (dále jen „**DNSH**"). Zásada DNSH - „Do No Significant Harm" je ukotvena ve sdělení Komise „Zelená dohoda pro Evropu" (European Green Deal).

8.25 Poskytovatel je povinen v průběhu realizace a po dobu deseti let od ukončení realizace Projektu, poskytovat požadované informace a dokumentaci zaměstnancům nebo zmocněncům pověřených orgánů (Ministerstvo vnitra, Ministerstva průmyslu a obchodu, Ministerstva financí, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy, Evropské komisi) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci Projektu a poskytnout jim při provádění kontroly součinnost. Poskytovatel je zároveň povinen řádně uchovávat veškerou dokumentaci související s realizací Projektu včetně účetních dokladů podle českých právních předpisů nejméně po dobu 10 let od schválení závěrečné zprávy o Projektu. Pro vyloučení pochybností Smluvní strany uvádějí, že k výše uvedeným činnostem je Poskytovatel povinen pouze v nezbytně nutném rozsahu, tj. pouze ve vztahu k činnostem, které Objednatel nemůže provést sám či dokumentům, které Objednatel nemá k dispozici. Na Poskytovatele nelze přenášet zákonné povinnosti vyplývající přímo pro Objednatele.

IX. ZMĚNOVÉ ŘÍZENÍ

9.1 Kterákoliv ze Smluvních stran je oprávněna na základě Zprávy písemně navrhnout změny v rozsahu a úrovni poskytovaných Služeb, a to prostřednictvím požadavku zaslaného Oprávněné osobě příslušné Smluvní strany (dále jen „**Změnový požadavek**"). Vzor Změnového požadavku je součástí Přílohy č. 2 Rámcové smlouvy. Žádná ze Smluvních stran není povinna navrhované změny akceptovat.

9.2 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.

9.3 Smluvní strany se zavazují za účelem potvrzení změn dle tohoto článku uzavřít dodatek k Rámcové smlouvě, resp. Objednávce, kterým budou provedené změny do Rámcové smlouvy, resp. Objednávky promítnuty. V závislosti na takovém dodatku může být upraven požadovaný rozsah plnění Služeb, termíny plnění Služeb, cena Služeb, platební podmínky, součinnost Objednatele atd.

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

X. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

10.1 Poskytovatel se zavazuje:

10.1.1 poskytovat Služby v kvalitě definované v konkrétní Objednávce;

10.1.2 poskytovat Služby řádně a včas bez faktických a právních vad;

10.1.3 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;

10.1.4 bez zbytečného odkladu oznámit Objednateli veškeré skutečnosti, které mohou mít vliv na povahu nebo na podmínky poskytování Služeb dle Rámcové smlouvy a Objednávek;

10.1.5 informovat bezodkladně Objednatele o všech okolnostech důležitých pro řádné a včasné plnění Rámcové smlouvy a Objednávek;

10.1.6 poskytnout Objednateli veškerou nezbytnou součinnost k naplnění účelu Rámcové smlouvy i všech Objednávek na jejím základě uzavřených;

10.1.7 nakládat se všemi věcmi, dokumenty a dalšími písemnostmi, které mu byly Objednatelem svěřeny za účelem plnění této Rámcové smlouvy a Objednávek, s péčí řádného hospodáře a chránit je před poškozením, a zneužitím. Objednatel zůstává vlastníkem takových podkladů poskytnutých Poskytovateli za účelem plnění této Rámcové smlouvy a Objednávek. Poskytovatel je oprávněn s podklady nakládat pouze v souladu s podmínkami této Rámcové smlouvy a Objednávek. 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 Rámcové smlouvy, a to nejpozději do 5 pracovních dnů od ukončení poslední Objednávky uzavřené na základě této Rámcové smlouvy, nedohodnou-li se Smluvní strany jinak;

10.1.8 mít po celou dobu účinnosti Rámcové smlouvy a jednotlivých Objednávek uzavřenou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Poskytovatelem v souvislosti s poskytováním Služeb Objednateli, příp. třetí osobě s limitem pojistného plnění minimálně ve výši 60 000 000 Kč;

10.1.9 poskytovat plnění dle Rámcové smlouvy a Objednávek sám nebo prostřednictvím poddodavatelů. Poskytovatel se zavazuje písemně informovat Objednatele o všech svých poddodavatelích a o jejich změně. Poskytovatel se zavazuje zajistit, že případným využitím poddodavatelů nedojde k porušení ZZVZ, zejména ustanovení § 11. 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;

10.1.10 poskytnout Služby dle této Rámcové smlouvy na své náklady a na své nebezpečí.

10.2 Objednatel se zavazuje:

10.2.1 poskytovat Poskytovateli úplné, pravdivé a včasné informace potřebné k řádnému a včasnému poskytování Služeb;

10.2.2 poskytovat Poskytovateli součinnost potřebnou pro řádné a včasné realizování Služeb, kterou je po něm Poskytovatel jako osoba, která disponuje kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci Služeb s odbornou péčí, oprávněna požadovat;

10.2.3 zaplatit za řádně poskytnuté Služby nebo jejich části cenu za Služby dle příslušné Objednávky;

10.2.4 v objektech v Místech plnění dodržovat veškeré obecně platné předpisy týkající se bezpečnosti a ochrany zdraví při práci a požární ochrany (BOZP a PO) a dále vnitřní předpisy Poskytovatele, se kterými byl Poskytovatelem prokazatelně seznámen, a provádět činnosti tak, aby nebyl v nadbytečném rozsahu omezen provoz na pracovištích Poskytovatele;

10.2.5 provést řádné seznámení všech svých zaměstnanců a případných jiných osob podílejících se na poskytování Služeb prostřednictvím Objednatele se zvláštními bezpečnostními a požárními opatřeními a zvláštními předpisy platnými pro objekt, do kterého Objednatel bude vstupovat v souvislosti s poskytováním Služeb a bude nést plnou odpovědnost za případné porušení výše uvedených opatření a předpisů Pracovníky Objednatele;

10.2.6 že pracovníci Objednatele budou při plnění této Rámcové smlouvy a Objednávek dodržovat obecně závazné právní předpisy, vztahující se k vykonávané činnosti, a budou se řídit organizačními pokyny Objednatele;

10.2.7 nejméně 2 (dva) pracovní dny před započetím s poskytováním Služeb předat Poskytovateli seznam pracovníků Objednatele, kteří budou vstupovat do Místa plnění a budou seznámeni s prostorem Místa plnění, do kterého budou moci vstupovat, přičemž vstupovat do Místa plnění jsou oprávněny pouze osoby schválené Poskytovatelem (dále jen „**Pracovníci Objednatele**"). V případě změny osob, které budou vstupovat do Místa plnění, je Objednatel povinen postupovat obdobně. Objednatel je povinen zajistit, aby do Místa plnění nevstupovaly osoby, které nebyly zapsány na výše uvedeném seznamu.

10.2.8 Poskytovatel dohodne s Objednatelem rozsah oprávnění Objednatele ke vstupu, a případně též k vjezdu, do objektů, ve kterých se nachází Místo plnění. Poskytovatel se zavazuje zajistit Objednateli doprovod Oprávněné osoby Poskytovatele.

10.2.9 u vstupu do objektu Poskytovatele, ve kterém se nachází Místo plnění zajistit vyčkání Pracovníků Objednatele na doprovod Oprávněné osoby Poskytovatele. Bez přítomnosti Oprávněné osoby Poskytovatele nejsou Pracovníci Objednatele oprávněni pohybovat se po objektu Poskytovatele, ve kterém se nachází místo plnění.

10.2.10 V případě vstupu do DCV a DCZ je Objednatel povinen dodržovat zejména Provozní řád pro návštěvníky datového centra (dále jen „Provozní řád BDC"). Objednatel je povinen dodržovat i jakékoliv budoucí aktualizované verze Provozního řádu BDC za předpokladu, že s nimi bude prokazatelně seznámen v souladu. Ustanovení Provozního řádu BDC mají přednost před pododst. 10.2.7, 10.2.8 a 10.2.9 tohoto odstavce Smlouvy.

XI. KYBERNETICKÁ BEZPEČNOST

11.1 Poskytovatel se zavazuje při plnění této Rámcové 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.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

11.2 Poskytovatel bere na vědomí, že Služby dle této Rámcové smlouvy souvisí s provozem, užitím, správou, či rozvojem kritické informační infrastruktury ve smyslu ustanovení § 2 písm. b) ZoKB.

11.3 Poskytovatel bere na vědomí, že v souvislosti se Službami dle této Rámcové smlouvy se stává Významným dodavatelem ve smyslu ustanovení § 2 písm. n) VoKB.

11.4 V případě kybernetického bezpečnostního incidentu (dále též „KBI") vzniklého v rámci poskytování Služeb, se Poskytovatel zavazuje tento KBI neprodleně oznámit v souladu s definovanými povinnostmi povinné osoby dle ZoKB a o tomto oznámení neprodleně informovat Objednatele (v postavení správce) 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 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 Objednatel bude ve věcech kybernetické bezpečnosti zastupovat Manažer kybernetické bezpečnosti Objednatele. Poskytovatel se zavazuje umožnit Objednateli provést kontrolu procesu odstraňování KBI a vypořádat se s případnými připomínkami Objednatele k procesu odstraňování KBI.

11.5 Kontrola zavedení a užití bezpečnostních opatření a procesů:

11.5.1 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 dle odst. 11.6 pododst. 11.6.1. Výzva na Poskytovatele bude zaslána minimálně 1 (jeden) měsíc před první takovou kontrolou. Poskytovatel v této věci poskytne Objednateli, nebo jím určené třetí straně, nutnou součinnost. Z kontroly vyhotoví Objednatel dokument s názvem „Zápis z kontroly Poskytovatele služby" (dále též „Zápis");

11.5.2 Při každé kontrole bude vždy přihlédnut o k rozsahu plnění dle rozsahu pověření dle ustanovení § 8 Řízení dodavatelů, odst. 1 písm. a) VoKB. 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. Poskytovatel vyhotoví písemné stanovisko k tomuto Zápisu do deseti pracovních dnů od doručení Zápisu a ve stejné lhůtě předloží toto stanovisko k projednání Oprávněné osobě Objednatele.

11.6 Poskytovatel je dále povinen:

11.6.1 dodržovat při poskytování Služby příslušná ustanovení bezpečnostních politik, metodik a postupů předaných Poskytovateli Objednatelem, resp. platné řídící dokumentace Objednatele či její části a/nebo platné řídící dokumentace, k jejímuž dodržování se Objednatel zavázal, pokud byl Poskytovatel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací Objednatele seznámen (např. školením, protokolárním předáním příslušné dokumentace Poskytovateli, elektronickým předáním prostřednictvím e-mailu, zřízením přístupu Poskytovateli na sdílené úložiště aj.). V případě provedených změn v bezpečnostní dokumentaci KII / VIS (dle relevance), bude Poskytovatel informován. Poskytovatel je povinen řídit se novým obsahem bezpečnostní dokumentace KII / VIS (dle relevance) od data stanoveného Objednatelem, nejdříve však ode dne, kdy byl o změně informován. Poskytovatel se dále zavazuje k zavedení a dodržování veškerých souvisejících bezpečnostních opatření požadovaných ZoKB a VoKB, a to minimálně po dobu poskytování plnění dle podmínek této Rámcové smlouvy;

11.6.2 informovat neprodleně Objednatele o kybernetických bezpečnostních incidentech a kybernetických bezpečnostních událostech na straně Poskytovatele souvisejících s plněním dle této Rámcové smlouvy. Kybernetická bezpečnostní událost je definována v ustanovení § 7 odst. 1 ZoKB a kybernetický bezpečnostní incident je definován ustanovením § 7 odst. 2 ZoKB;

11.6.3 informovat neprodleně Objednatele o změně ovládání Poskytovatele dle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s aktivy určenými k plnění dle této Rámcové smlouvy.

11.7 Poskytovatel je při poskytování Služby pro Objednatele oprávněn užívat data předaná Poskytovateli Objednatelem za účelem plnění předmětu Rámcové smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Rámcové smlouvy.

11.8 Poskytovatel se při poskytování plnění pro Objednatele zavazuje nakládat s daty pouze v souladu s Rámcovou smlouvou a příslušnými právními předpisy, zejména ZoKB, VoKB a dalšími souvisejícími právními předpisy.

11.9 Poskytovatel bere na vědomí, že přístup k datům, informacím či zařízením souvisejícím s předmětem Rámcové smlouvy je možné povolit pouze fyzické identitě zaměstnance Poskytovatele nebo subdodavatele Poskytovatele zaevidované v seznamu oprávněných osob, a to na základě požadavku Poskytovatele na přístup.

11.10 Poskytovatel bere na vědomí, že Objednatel může určit typ, rozsah, strukturu formátu dat, které Poskytovatel předá Objednateli; nedohodne-li se Objednatel s Poskytovatelem jinak, budou data Objednatele Poskytovatelem předána ve strukturovaném, běžně používaném, strojově čitelném a interoperabilním formátu. Objednatel určí lhůty k předání nebo zpřístupnění dat Objednatele a také dobu, po kterou budou případně data uschovaná Poskytovatelem po ukončení Rámcové smlouvy.

11.11 Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci Poskytovatele musí být řízeno zásadou tzv. „potřeba vědět" (need to know) a není nárokové.

11.12 Poskytovatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Poskytovatele nebo subdodavatele Poskytovatele.

11.13 Poskytovatel se zavazuje, že nebude instalovat a používat žádné nástroje, které nebyly předem písemně odsouhlaseny Objednatelem a jejichž užívání by mohlo ohrozit kybernetickou bezpečnost.

11.14 Poskytovatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému nebo nelegální získání dat a informací. Poskytovatel bere na vědomí, že přístup do interní sítě a/nebo k technologickým a komunikačním systémům bude realizován s využitím zařízení Objednatele. V případě, že Objednatel povolí Poskytovateli přístup do interní sítě a/nebo k technologickým a komunikačním systémům Objednatele ze zařízení Poskytovatele, musí veškerá tato zařízení Poskytovatel splňovat příslušné bezpečnostní standardy Objednatele.

11.15 Poskytovatel se během poskytování Služby pro Objednatele zavazuje dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, dostupnost a integritu.

11.16 Poskytovatel se zavazuje plnit požadavky Objednatele v oblasti likvidace dat (ať už dat na papírových médiích, dat zpracovávaných elektronicky nebo prostřednictvím jakýchkoliv dalších nosičů dat) dle přílohy č. 4 VoKB. Specifické provozní údaje, tedy bezpečnostní a provozní logy, včetně jejich záloh, budou vymazány v prostředí služby uplynutím lhůty platné pro IS KII. Výmaz dat Objednatele a specifických provozních údajů bude proveden způsobem znemožňujícím jejich obnovení forenzními postupy. Poskytovatel provádí bezpečnou likvidaci kryptografických klíčů, které šifrují obsah dat Objednatele v úložištích, v souladu s VoKB.

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

11.17 Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování Služby Objednateli, kteří přistupují do interní sítě a/nebo technologického nebo komunikačního systému, chránily autentizační prostředky a údaje k systémům Objednatele. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu platí pro Poskytovatele, pokud byl s takovou řídící dokumentací Objednatele seznámen).

11.18 Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či skutečnost vzniklá v důsledku porušení bezpečnostních požadavků nebude posuzována jako okolnost vylučující odpovědnost Poskytovatele za prodlení s řádným a včasným plněním předmětu Rámcové smlouvy a nebude důvodem k jakékoli náhradě případné újmy Poskytovateli či jiné osobě ze strany Objednatele. Ostatní ustanovení ohledně odpovědnosti Poskytovatele za prodlení obsažená v Rámcové smlouvě nejsou tímto ustanovením dotčena.

11.19 Poskytovatel se zavazuje poskytnout Objednateli veškerou nezbytnou součinnost ke splnění povinností Objednatele zejména při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.

11.20 Poskytovatel se zavazuje informovat Objednatele o způsobu řízení rizik na straně Poskytovatele a o zbytkových rizicích souvisejících s plněním Rámcové smlouvy.

11.21 Poskytovatel se zavazuje dodržovat požadavky Objednatele na řízení kontinuity činností.

11.22 Poskytovatel akceptuje, že veškeré náklady, které mu v průběhu plnění dle této Rámcové 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.

11.23 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 Rámcové smlouvy, má Poskytovatel povinnost toto bezpečnostní opatření zavést či užívat, nebo Objednateli poskytnout nutnou součinnost k zajištění uložených povinností.

11.24 V případě externího vývoje služby nebo jednotlivých technických aktiv jsou mezi Poskytovatelem a dodavatelem externího vývoje smluvně upraveny specifikace týkající se zejména:

11.24.1 bezpečnosti při vývoji softwaru v souladu s uznávanými standardy a metodami;

11.24.2 akceptačních testů kvality služeb poskytovaných v souladu s dohodnutými funkčními a nefunkčními požadavky;

11.24.3 poskytnutí důkazu o tom, že bylo provedeno dostatečné bezpečnostní ověření, aby se vyloučila existence známých zranitelností.

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 Rámcové smlouvy a Objednávek 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 Rámcové smlouvy bude postupovat tak, aby nedošlo k neoprávněnému zásahu do práv třetích osob.

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

12.5 Dojde-li při poskytování Služeb dle této Rámcové 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), poskytuje Poskytovatel Objednateli k takovému autorskému dílu, resp. databázi, nevýhradní oprávnění autorské dílo (včetně zdrojových kódů) užít, resp. databázi vytěžovat a zužitkovat, dle účelu této Rámcové 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. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

13.1 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 Rámcové smlouvy a Objednávek.

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

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

13.4 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.

XIV. ZÁRUKA A ODPOVĚDNOST ZA VADY

14.1 Poskytovatel poskytuje ve smyslu § 2619 Občanského zákoníku záruku za jakost na to, že předané výstupy z plnění Odborných činností dle příslušné Objednávky budou plně způsobilé pro použití ke smluvenému účelu, odpovídající sjednané technické specifikaci a parametrům a podmínkám stanoveným Objednatelem v příslušné Objednávce a budou bez jakýchkoliv vad a nedodělků. Záruka se vztahuje na všechny části výstupů příslušného plnění Odborných činností včetně jejich příslušenství a pokrývá všechny jejich součásti, včetně produktů třetích stran, které byly využity při realizaci příslušného plnění Odborných činností. Záruční doba počíná běžet dnem podpisu příslušného Akceptačního protokolu, popř. Výkazu Konzultací bez výhrad dle Rámcové smlouvy podepsaného oběma Smluvními stranami a skončí uplynutím 12 měsíců od tohoto okamžiku.

14.2 Poskytovatel odpovídá za jakoukoliv vadu výstupů z plnění Odborných činností, jež se vyskytne v době trvání záruky, pokud není způsobena zaviněním Objednatele z důvodu porušení jeho povinnosti. Záruční doba neběží po dobu, po kterou Objednatel nemůže užívat výstupy z Odborných činností, za které odpovídá Poskytovatel. Ustanovení § 2618 Občanského zákoníku Smluvní strany vylučují.

14.3 Objednatel je oprávněn uplatnit vady u Poskytovatele kdykoliv během záruční doby bez ohledu na to, kdy Objednatel takové vady zjistil nebo mohl zjistit. Pro vyloučení pochybností se sjednává, že převzetím jednotlivých částí výstupů Odborných činností není dotčeno právo Objednatele uplatňovat práva z vad, které byly zjistitelné, ale nebyly zjištěny při převzetí.

14.4 Poskytovatel je odpovědný za to, že Cloudové služby poskytne v souladu s Rámcovou smlouvou, resp. danou Objednávkou, a že po dobu trvání Rámcové smlouvy, resp. Objednávky budou mít dohodnuté vlastnosti, úroveň a charakteristiky.

14.5 Poskytovatel je povinen poskytovat Služby v nejvyšší dostupné kvalitě a odpovídá za to, že případné vady Služeb řádně odstraní, případně nahradí Službami bezvadnými v souladu s Rámcovou smlouvou, resp. Objednávkou.

14.6 Jakékoliv vady Odborných činností, které vzniknou v záruční době, je Poskytovatel povinen odstranit na své náklady v rámci poskytovaných Cloudových služeb dle Rámcové smlouvy, a to způsobem v Rámcové smlouvě uvedeným.

14.7 Pokud k jakékoliv části Služeb dle této Rámcové smlouvy nejsou poskytovány Provozní služby, nedohodnou-li se Smluvní strany jinak, je Poskytovatel povinen jakoukoliv záruční vadu takové části Služeb dle Rámcové smlouvy odstranit nejpozději do 10 pracovních dnů od doručení oznámení vady Objednatelem Poskytovateli, nedohodnou-li se Smluvní strany na delší lhůtě.

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

XV. NÁHRADA ÚJMY

15.1 Smluvní strany sjednávají, že náhrada újmy se bude řídit právními předpisy, není-li ve Rámcové smlouvě sjednáno jinak.

15.2 Smluvní strany odpovídají (v limitech dle odst. 15.3 tohoto článku) za každé zaviněné porušení smluvní povinnosti.

15.3 Smluvní strany se dohodly, že omezují právo na náhradu újmy, která může při plnění Rámcové smlouvy jedné Smluvní straně vzniknout, a to na celkovou částku odpovídající částce 64 000 000 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.

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

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

15.6 Žádná ze Smluvních stran není povinna nahradit újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Smluvní strany.

15.7 Žádná ze Smluvních stran nemá povinnost nahradit újmu způsobenou porušením svých povinností vyplývajících z této Rámcové smlouvy, bránila-li jí v jejich splnění některá z překážek vylučujících povinnost k náhradě škody ve smyslu § 2913 odst. 2 Občanského zákoníku.

XVI. MLČENLIVOST A OCHRANA INFORMACÍ SMLUVNÍCH STRAN

16.1 Obě Smluvní strany se zavazují, že zachovají 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:

16.1.1 veškeré informace poskytnuté si Smluvními stranami v souvislosti s plněním této Rámcové smlouvy či Objednávek (pokud nejsou výslovně obsaženy ve znění Rámcové smlouvy či Objednávky zveřejňovaném dle čl. XIX odst. 19.6);

16.1.2 informace, na které se vztahuje zákonem uložená povinnost mlčenlivosti;

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

16.2 Povinnost zachovávat mlčenlivost uvedená v odst. 16.1 tohoto článku se nevztahuje na informace:

16.2.1 které je Objednatel nebo Poskytovatel povinen poskytnout třetím osobám podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů;

16.2.2 jejichž sdělení vyžaduje jiný právní předpis;

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

16.2.4 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;

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

16.3 Jako s Neveřejnými informacemi musí být nakládáno také s informacemi, které splňují podmínky uvedené v odst. 16.1. 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 Rámcové smlouvy či Objednávek.

16.4 Smluvní strany se zavazují, že Neveřejné informace užijí pouze za účelem plnění této Rámcové smlouvy a Objednávek. K jinému užití je zapotřebí písemného souhlasu druhé Smluvní strany.

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

16.6 Povinnost mlčenlivosti dle této Rámcové smlouvy trvá i po naplnění této Rámcové smlouvy bez ohledu na zánik ostatních závazků z Rámcové smlouvy, a to v případě Neveřejných informací po dobu 5 let ode dne ukončení poslední Objednávky uzavřené na základě této Rámcové smlouvy a v případě obchodního tajemství po dobu existence obchodního tajemství, pokud nebude povinnosti mlčenlivosti dříve daná Smluvní strana druhou Smluvní stranou písemně zproštěna.

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

16.8 Poskytovatel se zavazuje zajistit při plnění Rámcové smlouvy a Objednávek ochranu osobních údajů, ke kterým má přístup. Smluvní strany se zavazují postupovat v souvislosti s plněním Rámcové smlouvy, resp. Objednávek v souladu s platnými a účinnými právními předpisy na ochranu osobních údajů, tj. zejména podle Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Pokud bude Smluvní strana v souvislosti s plněním Rámcové smlouvy, resp. Objednávek zpracovávat osobní údaje zaměstnanců/kontaktních osob/jiných dotčených osob druhé Smluvní strany, zavazuje se zpracovávat tyto osobní údaje pouze v rozsahu nezbytném pro plnění Rámcové smlouvy, resp. Objednávek a po dobu nezbytnou k plnění Rámcové smlouvy, resp. Objednávek. Jestliže Smluvní strany budou zpracovávat osobní údaje zaměstnanců nebo dalších dotčených osob druhé Smluvní strany nad rámec specifikovaný v této Rámcové smlouvě nebo po dobu delší, než je uvedeno v této Rámcové smlouvě, jsou povinny uzavřít samostatnou smlouvu o zpracování osobních údajů.

XVII. SANKCE

17.1 V případě prodlení Poskytovatele s povinností mít po celou dobu trvání Rámcové smlouvy uzavřenou pojistnou smlouvu dle čl. X odst. 10.1 pododst. 10.1.8 Rámcové smlouvy, má Objednatel právo uplatnit vůči Poskytovateli smluvní pokutu ve výši 50 000 Kč, a to každý započatý kalendářní den prodlení.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

17.2 V případě, že některá ze Smluvních stran poruší některou z povinností mlčenlivosti dle čl. XVI této Rámcové smlouvy, je druhá Smluvní strana oprávněna požadovat smluvní pokutu ve výši 100 000 Kč, a to každý jednotlivý případ porušení.

17.3 V případě, že některá ze Smluvních stran poruší některou z povinností dle čl. XIX odst. 19.10 této Rámcové smlouvy, je druhá Smluvní strana oprávněna požadovat smluvní pokutu ve výši 100 000 Kč, a to každý jednotlivý případ porušení.

17.4 V případě, že Poskytovatel nesplní některou ze stanovených dostupností uvedených v dané Objednávce je Objednatel oprávněn požadovat smluvní pokutu ve výši stanovené v dané Objednávce.

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

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

17.7 Ujednáním o smluvní pokutě není dotčeno právo poškozené Smluvní strany domáhat se náhrady škody v mezích dle odst. 15.3. Rámcové smlouvy.

17.8 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 Rámcovou smlouvou, resp. jednotlivými Objednávkami jedné Smluvní straně se omezuje částkou 23 000 000 Kč.

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

XVIII. DOBA TRVÁNÍ RÁMCOVÉ SMLOUVY A UKONČENÍ RÁMCOVÉ SMLOUVY A OBJEDNÁVEK

18.1 Rámcová smlouva se uzavírá na dobu určitou, tj. na dobu 48 měsíců od účinnosti Rámcové smlouvy nebo do okamžiku, kdy celková hodnota plnění uzavřených Objednávek dosáhne Maximální souhrnné ceny, podle toho, která ze skutečností nastane dříve.

18.2 Rámcovou smlouvu i jednotlivé Objednávky lze ukončit písemnou dohodou Smluvních stran podepsanou osobami oprávněnými jednat za Smluvní strany, přičemž účinky ukončení Rámcové smlouvy, resp. Objednávky nastanou k okamžiku stanovenému v takové dohodě.

18.3 Platnost nebo účinnost Rámcové smlouvy není nijak závislá na platnosti nebo účinnosti Objednávek a zároveň platnost a účinnost Objednávek uzavřených do konce účinnosti Rámcové smlouvy není nijak závislá na platnosti a účinnosti Rámcové smlouvy. Aniž by byla dotčena předcházející věta, Smluvní strany výslovně sjednávají, že jednotlivé Objednávky lze uzavírat s koncem účinnosti nejpozději k datu uplynutí 48 měsíců od okamžiku účinnosti Rámcové smlouvy.

18.4 Každá ze Smluvních stran je oprávněna Rámcovou smlouvu a každou jednotlivou Objednávku na Cloudové služby či Služby KB vypovědět, a to i bez udání důvodu a včetně těch Objednávek na Cloudové služby či Služby KB, které jsou uzavřené na dobu určitou. Výpovědní doba Rámcové smlouvy činí 6 měsíců a počíná běžet prvním dnem měsíce následujícího po měsíci, ve kterém bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé Smluvní straně. Výpovědní doba předmětných Objednávek činí 3 měsíce, pokud nebude v předmětné Objednávce stanovena doba delší a počíná běžet prvním dnem měsíce následujícího po měsíci, ve kterém bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé Smluvní straně.

18.5 Rámcová smlouva či Objednávky mohou zaniknout odstoupením příslušné Smluvní strany, nastanou-li okolnosti předvídané § 2002 OZ.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

18.6 Odstoupením se závazek založený touto Rámcovou smlouvou, příp. danou Objednávkou zrušuje pouze ohledně nesplněného zbytku plnění (tj. ex nunc). Smluvní strany si jsou povinny vyrovnat dosavadní vzájemné závazky z Rámcové smlouvy, příp. Objednávky, a to bez zbytečného odkladu, nejpozději však do 30 dnů od doručení oznámení Smluvní strany o odstoupení od Rámcové smlouvy, příp. Objednávky druhé Smluvní straně. Aniž by byla dotčena předchozí věta, zůstávají závazky vyplývající z Objednávek uzavřených Objednatelem a Poskytovatelem do okamžiku účinnosti odstoupení od Rámcové smlouvy nedotčeny.

18.7 Za podstatné porušení Rámcové smlouvy a rovněž příslušné Objednávky Poskytovatelem se považuje zejména jednání, kdy je Poskytovatel v prodlení s poskytováním příslušné Služby dle příslušné Objednávky o více než 30 kalendářních dnů.

18.8 Objednatel je dále oprávněn od Rámcové smlouvy, resp. Objednávek odstoupit v případě, že:

18.8.1 bude rozhodnuto o likvidaci Poskytovatele;

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

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

18.8.4 Poskytovatel se stane Nespolehlivým plátcem;

18.8.5 dojde k významné změně kontroly nad Poskytovatelem, 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;

18.8.6 dojde ke změně kontroly nad zásadními aktivy využívanými Poskytovatelem k plnění podle Smlouvy;

18.8.7 v případě změny skutečného majitele Poskytovatele podle zákona č. 37/2021 Sb., o evidenci skutečných majitelů, ve znění pozdějších předpisů; za změnu skutečného majitele se pro účely tohoto pravidla nepovažuje změna osoby ve vrcholovém vedení Poskytovatele;

18.8.8 v případě změny sídla Poskytovatele do jiné země mimo území EU/EHP;

18.8.9 v případě vydání opatření NÚKIB podle ZoKB ve vztahu k Poskytovateli nebo poddodavateli nebo jakékoliv části Služeb;

18.8.10 dojde-li k výmazu Poskytovatele z katalogu cloud computingu z důvodu neplnění požadavků na poskytovatele cloud computingu podle zákona č. 365/2000 Sb.;

18.8.11 v případě změny poddodavatele bez souhlasu Objednatele;

18.8.12 v případě změny kontroly nad zásadními podpůrnými aktivy ve smyslu VoKB využívanými Poskytovatelem k poskytování Služeb;

18.8.13 v případě, že nastane významná změna v poskytování Služeb, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko.

18.9 Nastane-li některý z případů uvedených v odst. 18.8 tohoto článku Rámcové smlouvy, je Poskytovatel povinen informovat o této skutečnosti Objednatele písemně do 2 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 Rámcové smlouvy, příp. Objednávky. Nedodržení této povinnosti je podstatným porušením Rámcové smlouvy.

18.10 Dosáhne-li plnění z této Rámcové smlouvy takové výše, že Služby není možné provést bez překročení Maximální souhrnné ceny, má každá Smluvní strana právo od Rámcové smlouvy odstoupit. Ustanovení odst. 18.12 tohoto článku se použije obdobně.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

18.11 Za podstatné porušení Rámcové smlouvy a rovněž příslušné Objednávky Objednatelem ve smyslu § 2002 OZ se považuje zejména prodlení Objednatele s úhradou faktury o více než 30 kalendářních dnů.

18.12 Odstoupení od Rámcové smlouvy, jakož i Objednávky 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 Rámcové smlouvy nebo Objednávky 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.

18.13 V případě jakéhokoliv ukončení Rámcové smlouvy je Poskytovatel postupem stanoveným pro plnění Ostatních činností, tj. na základě požadavku Objednatele, povinen poskytnout Objednateli nebo Objednatelem určené třetí osobě maximální nezbytnou součinnost za účelem plynulého a řádného převedení činností dle Rámcové smlouvy, resp. Objednávek účinných ke dni ukončení Rámcové smlouvy či jejich části na Objednatele nebo Objednatelem určenou třetí osobu tak, s výjimkou případu, že by novým poskytovatelem Služeb byl stávající Poskytovatel dle této Rámcové smlouvy, aby Objednateli nevznikla újma (škoda) související s přechodem poskytování Služeb dle této Rámcové smlouvy na nového poskytovatele Služeb. Poskytovatel se zavazuje tuto součinnost poskytovat s odbornou péčí, zodpovědně v rozsahu, který po něm lze spravedlivě požadovat, a to do doby úplného převzetí takových činností Objednatelem nebo Objednatelem určenou třetí osobou. Součinnost bude spočívat především ve vykonání plánu předání (dále jen „**Exit plán**"). Činnosti vedoucí k řádnému vykonání Exit plánu proběhnou dle následujících pravidel a v následujícím rozsahu:

18.13.1 Pět měsíců před účinností ukončení Rámcové smlouvy vznikne společná pracovní skupina Poskytovatele a Objednatele, zahrnující zástupce obou stran z oblasti technické, ekonomické i právní;

18.13.2 pracovní skupina vytvoří Exit plán, který bude nejpozději čtyři měsíce před termínem ukončení Rámcové smlouvy schválen oběma Smluvními stranami;

18.13.3 neschválení Exit plánu v uvedeném termínu bude řešeno do 10 pracovních dnů na jednání Oprávněných osob Objednatele i Poskytovatele;

18.13.4 Exit plán musí obsahovat činnosti provozního, dokumentačního a školicího charakteru, včetně předávání znalostí a podpory migrace, související s předmětem a rozsahem Služeb;

18.13.5 v období 3 měsíců před ukončením Rámcové smlouvy budou oběma Smluvními stranami vykonávány činnosti obsažené v Exit plánu.

18.14 Výše uvedené termíny v odst. 18.13 neplatí v případě, pokud termín ukončení Rámcové smlouvy není znám alespoň šest měsíců dopředu, pak bude tato součinnost poskytována v termínech určených Objednatelem; její poskytování bude ukončeno nejpozději do konce třetího měsíce od ukončení Rámcové smlouvy.

18.15 Cena za Exit plán bude Objednatelem vypočtena na základě Ceny za Ostatní činnosti, kdy bude předem Objednatelem v Objednávce stanoven maximální počet člověkodní za provedení činností souvisejících s Exit plánem.

18.16 V případě, že za účelem vykonání Exit plánu bude nutné provést export dat z cloudového prostředí Poskytovatele do jiného prostředí, sjednávají Smluvní strany, že tento rozsah služeb a jejich cena budou součástí samostatného smluvního vztahu uzavřeného mimo rámec plnění této Rámcové smlouvy.

18.17 Ukončením Rámcové smlouvy, jakož i Objednávek nejsou dotčena práva na zaplacení smluvní pokuty nebo zákonného úroku z prodlení, pokud už dospěl, práva na náhradu újmy, práva a povinnosti vyplývající z čl. XVI Rámcové smlouvy, práva z odpovědnosti za vady ani další ujednání, z jejichž povahy vyplývá, že mají zavazovat Smluvní strany i po zániku účinnosti této Rámcové smlouvy nebo Objednávky.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

XIX. ZÁVĚREČNÁ USTANOVENÍ

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

19.1.1 Objednatel:

Název: Česká republika – Ministerstvo pro místní rozvoj

Adresa: Staroměstské nám. 932/6, 110 00, Praha 1

K rukám: jméno Oprávněné osoby Objednatele

Datová schránka: 26iaava

19.1.2 Poskytovatel:

Název: Státní pokladna Centrum sdílených služeb, s. p.

Adresa: Na Vápence 915/14, 130 00 Praha 3

K rukám: jméno Oprávněné osoby Poskytovatele

Datová schránka: ag5uunk

19.2 Účinnost oznámení nastává v pracovní den následující po dni doručení tohoto oznámení druhé Smluvní straně, není-li v Rámcové smlouvě nebo Objednávce v konkrétním případě stanoveno jinak.

19.3 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 Rámcové smlouvy a Objednávek, s výjimkou změn Rámcové smlouvy formou dodatku k Rámcové smlouvě nebo ukončení Rámcové smlouvy, uzavření Objednávek, změn Objednávek formou dodatku k Objednávce či ukončení Objednávek a oznámení o změně bankovních údajů a s výjimkou činností svěřených dle této Smlouvy odlišným osobám, není-li v Rámcové 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:

19.3.1 Oprávněnými osobami Objednatele jsou:

19.3.2 Oprávněnými osobami Poskytovatele jsou:

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

[redacted]

19.4 Ke změně Rámcové smlouvy formou dodatku k Rámcové smlouvě nebo ukončení Rámcové smlouvy, k uzavření Objednávek, ke změně Objednávek formou dodatku k Objednávce či ukončení Objednávek a k oznámení o změně bankovních údajů je za Objednatele oprávněn ředitel odboru cestovního ruchu nebo osoba pověřená ministrem pro místní rozvoj. Ke změně Rámcové smlouvy formou dodatku k Rámcové smlouvě nebo ukončení Rámcové smlouvy, k uzavření Objednávek, ke změně Objednávek formou dodatku k Objednávce či ukončení Objednávek a k oznámení o změně bankovních údajů je za Poskytovatele oprávněn 1. zástupce generálního ředitele, 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.

19.5 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.

19.6 Obě Smluvní strany souhlasí s tím, že podepsaná Rámcová smlouva (včetně příloh) a Objednávky (vč. případných příloh), jakož i jejich text, můžou být v elektronické formě zveřejněny v souladu s povinnostmi vyplývajícími z právních předpisů, a to bez časového omezení. Poskytovatel se zavazuje, že Rámcovou smlouvu a Objednávky v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) (dále jen „**Zákon o registru smluv**") uveřejní v registru smluv.

19.7 Tato Rámcová smlouva a Objednávky se řídí OZ a dalšími příslušnými právními předpisy České republiky, není-li v Rámcové smlouvě stanoveno jinak.

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

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

19.10 Smluvní strany nejsou oprávněny bez předchozího písemného souhlasu druhé Smluvní strany postoupit Rámcovou smlouvu, jakož i Objednávky, jednotlivý závazek z Rámcové smlouvy či Objednávek ani pohledávky vzniklé v souvislosti s touto Rámcovou smlouvou nebo Objednávkou na třetí osoby, ani učinit jakékoliv právní jednání, v jehož důsledku by došlo k převodu nebo přechodu práv či povinností vyplývajících z této Rámcové smlouvy, jakož i Objednávek.

19.11 Změny nebo doplňky této Rámcové smlouvy včetně příloh a změny nebo doplňky Objednávek vč. příloh musejí být vyhotoveny písemně formou dodatku, datovány a podepsány oběma Smluvními stranami s podpisy Smluvních stran na jedné písemnosti, ledaže Rámcová smlouva či Objednávka v konkrétním případě stanoví jinak.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

19.12 Smluvní strany se dohodly, že veškeré spory vyplývající z této Rámcové smlouvy nebo Objednávek nebo spory o existenci této Rámcové smlouvy nebo Objednávek (včetně otázky vzniku a platnosti Rámcové smlouvy nebo Objednávek) 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.

19.13 Smluvní strany se dohodly, že v rámci této Rámcové smlouvy a Objednávek vylučují aplikaci § 557 OZ.

19.14 Tato Rámcová smlouva představuje úplnou dohodu mezi Smluvními stranami, která nahrazuje veškeré předchozí ujednání a závazky vztahující se k předmětu plnění této Rámcové smlouvy.

19.15 Rámcová smlouva nabývá platnosti dnem podpisu oběma Smluvními stranami a účinnosti dnem uveřejnění Rámcové smlouvy v registru smluv dle Zákona o registru smluv.

19.16 Rámcová smlouva je vyhotovena v elektronické podobě v 1 vyhotovení v českém jazyce 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.

19.17 Smluvní strany prohlašují, že se se zněním Rámcové smlouvy podrobně seznámily a že ji na důkaz své svobodné a určité vůle a nikoli pod nátlakem, níže uvedeného dne podepisují.

19.18 Nedílnou součástí této Rámcové smlouvy jsou následující přílohy:

Příloha č. 1 – Popis a ceník rolí pro poskytování Odborných činností

Příloha č. 2 – Vzory dokumentů

Příloha č. 3 – Odkazy na specifikaci Cloudových služeb a Ceny za Cloudové služby

Příloha č. 4 – Specifikace Služeb KB – Katalogové listy

Příloha č. 5 – Ceník Služeb kybernetické bezpečnosti

Za Objednatele:
V Praze dne dle el. podpisu

[redacted]
Ministerstvo pro místní rozvoj

Za Poskytovatele:
V Praze dne dle el. podpisu

[redacted]
Státní pokladna Centrum sdílených služeb, s. p.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Rámcová smlouva o poskytování Cloudových a dalších souvisejících služeb

Příloha č. 1 – Popis a ceník rolí pro poskytování Odborných činností

ID	Název Odborné role	Popis činností
1	Analytik KB	Provádí hloubkové analýzy kybernetických bezpečnostních událostí a incidentů (KBU a KBI). Provádí odborné konzultace (po technické stránce) v oblasti kybernetické bezpečnosti. Spolupracuje při vyšetřování kybernetických bezpečnostních událostí a incidentů. Komunikuje s odbornou veřejností při výměně zkušeností a sdílení informací týkajících se kybernetických útoků a způsobech zabezpečení. Zpracovává dokumentaci ve svěřené oblasti kybernetické bezpečnosti. Spolupracuje na analýze, sběru, dekompozici a syntéze získaných informací a na návrhu implementace Bezpečnostního monitoringu. Účastní se jednání s pracovníky Objednatele. Zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem. Provádí penetrační testy.
2	Architekt KB	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. Provádí analýzu, sběr, dekompozici a syntézu získaných informací a navrhuje implementaci bezpečnostního monitoringu. Zajišťuje prosazování bezpečnosti informací v rámci koncepčního 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.
3	Manažer KB	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.
4	Manažer řízení rizik KB	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.
5	Organizátor vzdělávacích aktivit KB	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

ID	Název Odborné role	Popis činností
		konzultace k vedení evidence záznamů o vzdělávání a přípravě návrhu roční zprávy o budování bezpečnostního povědomí.
6	Manažer rozvoje služeb KB	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.
7	Aplikační administrátor	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.
8	Datový analytik	Podílí se 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.
9	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.
10	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.
11	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.
12	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.
13	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

ID	Název Odborné role	Popis činností
		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.
14	IT analytik / IT architekt	Analýza požadavků a potřeb zákazníka pro IT systémy a infrastrukturu. Návrh a optimalizace IT architektury s ohledem na funkčnost, výkon, bezpečnost a škálovatelnost. Tvorba technických specifikací a dokumentace pro nové systémy a aplikace. Spolupráce s vývojovými týmy při implementaci IT řešení. Posouzení a doporučení technologií a nástrojů pro zlepšení IT infrastruktury. Monitorování a hodnocení výkonu IT systémů a navrhování opatření pro jejich optimalizaci. Řešení technických problémů a incidentů v oblasti IT architektury. Podpora při plánování a realizaci IT projektů, včetně migrací a integrací systémů. Zajištění souladu IT systémů s bezpečnostními standardy a předpisy. Školení a podpora uživatelů a IT personálu v oblasti nových technologií a systémů.
15	Manažer služeb	Správa a dohled nad plněním smluvních závazků v oblasti poskytovaných služeb. Koordinace a řízení týmů pro zajištění kvality služeb. Monitorování a hodnocení výkonu služeb podle smluvních parametrů. Řešení incidentů a problémů souvisejících s provozem služeb. Zajištění souladu služeb s bezpečnostními a regulačními požadavky. Příprava a prezentace pravidelných zpráv o plnění smluv a výkonnosti služeb. Identifikace a implementace opatření pro zlepšení efektivity a kvality služeb. Spolupráce s klienty na definování a aktualizaci požadavků a očekávání. Plánování a realizace rozvojových projektů v oblasti datového centra. Školení a podpora týmu v oblasti správy a optimalizace služeb.
16	Projektový manažer	Odpovídá za dodání všech projektových výstupů v požadovaném rozsahu, kvalitě a termínech a za dodržení schváleného rozpočtu projektu. Řídí svěřený projekt v souladu s projektovou metodikou SPCSS. Navrhuje schéma a obsazení projektových týmů. Stanovuje úkoly členům projektových týmů, následně kontroluje a dohlíží na jejich plnění. Koordinuje práci projektových týmů, určuje pravidla komunikace a spolupráce projektových týmů. Odpovídá za tvorbu a obsahovou správnost projektových dokumentů, vč. zápisů z jednání. Organizuje jednání s externími subjekty (zákazník, dodavatelé). Zpracovává písemné zprávy o stavu projektu, připravuje podklady pro smlouvy a veřejné zakázky mající vztah k projektu. Řídí rizika a změny projektu, eviduje a eskaluje kritická místa v projektu. Spolupracuje při přípravě návrhu nabídky pro požadované řešení zákazníka.
17	Procesní manažer/architekt	Analýza a mapování stávajících procesů a identifikace oblastí pro zlepšení. Návrh a implementace nových procesů a optimalizace stávajících s cílem zvýšit efektivitu a kvalitu. Spolupráce s různými odděleními na definování a dokumentaci procesních požadavků. Vytváření a udržování procesních map a dokumentace. Monitorování a hodnocení výkonnosti procesů a navrhování opatření pro jejich zlepšení. Řízení změn v procesech a zajištění jejich hladké implementace. Poskytování odborné podpory a školení zaměstnancům v oblasti procesního řízení. Zajištění souladu procesů s interními a externími předpisy a standardy. Identifikace a řízení rizik spojených s procesními změnami. Spolupráce na vývoji a implementaci nástrojů a technologií pro podporu procesního řízení.
18	Administrátor SAP	Správa a údržba SAP systémů, včetně instalace, konfigurace a aktualizace. Monitorování výkonu SAP systémů a zajištění jejich optimálního provozu. Řešení technických problémů a incidentů souvisejících se SAP systémy. Implementace a správa uživatelských účtů a přístupových práv v SAP. Zajištění souladu SAP systémů s bezpečnostními standardy a předpisy. Spolupráce s vývojáři a konzultanty na implementaci nových funkcionalit a modulů. Vytváření a udržování technické dokumentace SAP systémů. Provádění pravidelných záloh a obnovy dat v SAP systémech. Testování a nasazení

ID	Název Odborné role	Popis činností
		aktualizací a oprav SAP systémů. Poskytování technické podpory a školení uživatelům SAP systémů.
19	Obchodní manažer	Rozvoj a implementace obchodní strategie pro dosažení stanovených cílů. Identifikace nových obchodních příležitostí a rozšiřování zákaznické základny. Vedení a motivace obchodního týmu k dosažení prodejních cílů. Sledování a analýza tržních trendů a konkurence. Budování a udržování vztahů s klíčovými zákazníky a partnery. Příprava a prezentace obchodních nabídek a smluv. Vyjednávání podmínek a uzavírání obchodních smluv. Monitorování a hodnocení výkonnosti obchodního týmu a jednotlivých členů. Řešení problémů a stížností zákazníků s cílem zajistit jejich spokojenost. Příprava pravidelných zpráv o prodejních výsledcích a obchodních aktivitách.
20	Správce licencí	Správa a údržba licenčních smluv a zajištění jejich souladu s právními předpisy. Monitorování a evidence využívání softwarových licencí v organizaci. Zajištění optimálního využití licencí a minimalizace nákladů na software. Řešení problémů a incidentů souvisejících s licencemi. Spolupráce s dodavateli softwaru na nákupu a obnově licencí. Vytváření a udržování přehledné dokumentace o licencích a jejich využití. Poskytování odborné podpory a školení zaměstnancům v oblasti licencování. Provádění pravidelných auditů licencí a zajištění jejich souladu s interními a externími požadavky. Identifikace a implementace opatření pro zlepšení správy licencí. Sledování a analýza trendů v oblasti licencování a doporučování vhodných řešení.
21	Business analytik/architekt	Analýza a dokumentace obchodních požadavků a procesů. Návrh a architektura systémů odpovídajících obchodním potřebám. Spolupráce s vývojovými a technickými týmy na implementaci řešení. Průběžné hodnocení a optimalizace obchodních procesů a systémů. Plánování a řízení projektů zaměřených na zlepšení obchodních procesů. Spolupráce s klienty na definování a aktualizaci jejich požadavků a očekávání. Tvorba a údržba dokumentace k obchodním procesům a systémům. Poskytování školení a podpory uživatelům nových systémů a procesů. Zajištění souladu navrhovaných řešení s regulačními a bezpečnostními požadavky. Identifikace příležitostí pro inovace a zlepšení obchodních procesů a technologií.
22	Správce zranitelností	Zajišťuje provádění ad-hoc a pravidelného testování zranitelností při využití služby vulnerability management. Zajišťuje vyhledávání a ošetřování zranitelností v ICT v souladu s bezpečnostními požadavky ve spolupráci s administrátory IS při využití služby vulnerability management. Spravuje nastavení pravidelných skenů zranitelností. Podává podněty k řešení možných zjištěných hrozeb. Spolupracuje při vyšetřování kybernetických bezpečnostních událostí a incidentů. Zpracovává dokumentaci ve svěřené oblasti kybernetické bezpečnosti. Spolupracuje na analýze, sběru, dekompozici a syntéze získaných informací a na návrhu implementace služby vulnerability management. Účastní se jednání s pracovníky Objednatele. Zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem. Vykonává metodickou a konzultační činnost v oblasti vulnerability managementu a penetrační testy. Provádí penetrační testy.
23	Správce identit a integrací	Provádí odborné konzultace v oblasti správy privilegovaných účtů. Účastní se jednání s pracovníky Objednatele. Provádí vstupní analýzu před implementací správy privilegovaných účtů. Podílí se na všech jednotlivých úkonech spojených se správou privilegovaných účtů. Vytváří a reviduje dokumentaci související se správou privilegovaných účtů. Spolupracuje při vyšetřování kybernetických bezpečnostních událostí a incidentů. Provádí školení uživatelů Objednatele. Vytváří návody a postupy pro uživatele Objednatele. Zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Ceník rolí pro poskytování Odborných činností

ID	Role	Cena za 1 ČD v Kč bez DPH	DPH	Cena za 1 ČD v Kč včetně DPH	Cena za 1 ČH v Kč bez DPH	DPH	Cena za 1 ČH v Kč včetně DPH
1	Analytik KB	13 800,00	2 898,00	16 698,00	1 725,00	362,25	2 087,25
2	Architekt KB	17 700,00	3 717,00	21 417,00	2 212,50	464,63	2 677,13
3	Manažer KB	14 600,00	3 066,00	17 666,00	1 825,00	383,25	2 208,25
4	Manažer řízení rizik KB	12 800,00	2 688,00	15 488,00	1 600,00	336,00	1 936,00
5	Organizátor vzdělávacích aktivit KB	12 100,00	2 541,00	14 641,00	1 512,50	317,63	1 830,13
6	Manažer rozvoje KB	14 900,00	3 129,00	18 029,00	1 862,50	391,13	2 253,63
7	Aplikační administrátor	12 100,00	2 541,00	14 641,00	1 512,50	317,63	1 830,13
8	Datový analytik	11 800,00	2 478,00	14 278,00	1 475,00	309,75	1 784,75
9	Administrátor UNIX	14 100,00	2 961,00	17 061,00	1 762,50	370,13	2 132,63
10	Administrátor MS	13 000,00	2 730,00	15 730,00	1 625,00	341,25	1 966,25
11	Administrátor DB	15 400,00	3 234,00	18 634,00	1 925,00	404,25	2 329,25
12	Administrátor SAZ	14 400,00	3 024,00	17 424,00	1 800,00	378,00	2 178,00
13	Administrátor NET	13 900,00	2 919,00	16 819,00	1 737,50	364,88	2 102,38
14	IT analytik, IT architekt	14 900,00	3 129,00	18 029,00	1 862,50	391,13	2 253,63
15	Manažer služeb	13 600,00	2 856,00	16 456,00	1 700,00	357,00	2 057,00
16	Projektový manažer	13 600,00	2 856,00	16 456,00	1 700,00	357,00	2 057,00
17	Procesní manažer/architekt	12 100,00	2 541,00	14 641,00	1 512,50	317,63	1 830,13
18	Administrátor SAP	18 500,00	3 885,00	22 385,00	2 312,50	485,63	2 798,13
19	Obchodní manažer	12 400,00	2 604,00	15 004,00	1 550,00	325,50	1 875,50
20	Správce licencí	10 800,00	2 268,00	13 068,00	1 350,00	283,50	1 633,50
21	Business analytik/architekt	15 800,00	3 318,00	19 118,00	1 975,00	414,75	2 389,75
22	Správce zranitelností	12 500,00	2 625,00	15 125,00	1 562,50	328,13	1 890,63
23	Správce identit a integrací	13 600,00	2 856,00	16 456,00	1 700,00	357,00	2 057,00

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Rámcová smlouva o poskytování Cloudových a dalších souvisejících služeb

Příloha č. 2 – Vzory dokumentů

Seznam vzorů protokolů a formulářů obsažených v této příloze:

Objednávka –Cloudové služby/Služby KB

1. Záznam
2. Zpráva
3. Nabídka
4. Objednávka – Ostatní činnosti
5. Akceptační protokol
6. Objednávka – Konzultace
7. Výkaz Konzultací
8. Změnový požadavek

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

SPCSS Státní pokladna Centrum sdílených služeb

OBJEDNÁVKA

Cloudové služby/Služby KB

číslo **OBJYYYYXXX**

č. j. **SPCSS-xxxxx/20xx**

vystavena dne **[BUDE DOPLNĚNO]**

Objednatel		**Poskytovatel**	
Název	[BUDE DOPLNĚNO]	Název	[BUDE DOPLNĚNO]
Sídlo	[BUDE DOPLNĚNO]	Sídlo	[BUDE DOPLNĚNO]
	[BUDE DOPLNĚNO]		[BUDE DOPLNĚNO]
IČO	[BUDE DOPLNĚNO]	IČO	[BUDE DOPLNĚNO]
DIČ	[BUDE DOPLNĚNO]	DIČ	[BUDE DOPLNĚNO]
Vystavil	[BUDE DOPLNĚNO]	Rámcová smlouva	[BUDE DOPLNĚNO]
Na základě	[BUDE DOPLNĚNO]	Nabídka	[BUDE DOPLNĚNO]
Kontaktní os.	[BUDE DOPLNĚNO]	**Kontaktní os.**	[BUDE DOPLNĚNO]
Telefon	[BUDE DOPLNĚNO]	Telefon	[BUDE DOPLNĚNO]
E-mail	[BUDE DOPLNĚNO]	E-mail	[BUDE DOPLNĚNO]
Název plnění	[BUDE DOPLNĚNO]		

Objednatel objednává od Poskytovatele následující položky:

P. č.	Popis	Množství	MJ	Cena za jednotku v Kč bez DPH
1	Cloudové služby [BUDE DOPLNĚNO DLE POŽADOVANÉHO TYPU CLUDOVÝCH SLUŽEB Z KATALOGU CLOUDOVÝCH SLUŽEB]/ Služby KB (resp. PoC) [BUDE DOPLNĚNO DLE POŽADOVANÉHO TYPU SLUŽEB KB Z PŘÍLOHY Č. 4 RÁMCOVÉ SMLOUVY]	[BUDE DOPLNĚNO]	měsíc	[BUDE DOPLNĚNO]
2	[BUDE DOPLNĚNO DLE POŽADOVANÉHO TYPU CLUDOVÝCH SLUŽEB Z KATALOGU CLOUDOVÝCH SLUŽEB]/ [BUDE DOPLNĚNO DLE POŽADOVANÉHO TYPU SLUŽEB KB Z PŘÍLOHY Č. 4 RÁMCOVÉ SMLOUVY]	[BUDE DOPLNĚNO]	měsíc	[BUDE DOPLNĚNO]

Podrobná specifikace požadovaných Cloudových služeb / Služeb KB [BUDE DOPLNĚNO DLE POŽADOVANÉHO TYPU SLUŽBY]	[BUDE DOPLNĚNO]
Požadovaný termín zahájení	[BUDE DOPLNĚNO]
Požadovaný termín ukončení	[BUDE DOPLNĚNO]
Místo plnění	[BUDE DOPLNĚNO]
Poznámka	[BUDE DOPLNĚNO]
Přílohy	[BUDOU DOPLNĚNY JEDNOTLIVÉ KATALOGOVÉ LISTY]

Za Objednatele		**Za Poskytovatele**	
Jméno, příjmení	[BUDE DOPLNĚNO]	**Jméno, příjmení**	[BUDE DOPLNĚNO]

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Datum a podpis		**Datum a podpis**	
Upozorňujeme, že plnit Objednávku lze až po její řádné písemné akceptaci ze strany Poskytovatele s tím, že následně bude potvrzená Objednávka Objednatelem zveřejněna v Registru smluv v souladu s požadavky vyplývajícími ze zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) v platném znění.			

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

ZÁZNAM

Rámcová smlouva (dále jen „**Rámcová smlouva**")	[BUDE DOPLNĚNO]		
Objednatel (dále jen „**Objednatel**")	[BUDE DOPLNĚNO]		
Poskytovatel (dále jen „**Poskytovatel**")	[BUDE DOPLNĚNO]		
Vykazované období (dále jen „**Vykazované období**")	[BUDE DOPLNĚNO]		
Vypracoval	[BUDE DOPLNĚNO]	**Datum**	[BUDE DOPLNĚNO]

Obě Smluvní strany potvrzují, že v uvedeném období byly v souladu se Rámcovou smlouvou poskytnuty níže specifikované Cloudové služby/Služby KB v účtovaném množství

Cloudová služba/Služba KB – Objednávka č.	Cena za období v Kč bez DPH	**DPH v Kč**	Cena za období v Kč včetně DPH
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]
Celkem	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]

Detailní přehled poskytnutých Cloudových služeb bude uveden v měsíční Zprávě.

Schvalovací doložka

Jméno a příjmení	**Organizace**	**Datum a podpis**
[BUDE DOPLNĚNO]	Objednatel	[elektronický podpis včetně data podpisu]
[BUDE DOPLNĚNO]	Poskytovatel	[elektronický podpis včetně data podpisu]

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

ZPRÁVA

Rámcová smlouva (dále jen „**Rámcová smlouva**")	[BUDE DOPLNĚNO]		
Objednatel (dále jen „**Objednatel**")	[BUDE DOPLNĚNO]		
Poskytovatel (dále jen „**Poskytovatel**")	[BUDE DOPLNĚNO]		
Vykazované období (dále jen „**Vykazované období**")	[BUDE DOPLNĚNO]		
Vypracoval	[BUDE DOPLNĚNO]	**Datum**	[BUDE DOPLNĚNO]

Období a režim poskytování Cloudových služeb/Služeb KB
[BUDE DOPLNĚNO]
Rozsah poskytovaných Cloudových služeb/Služeb KB
[BUDE DOPLNĚNO]
Řešení závad
[BUDE DOPLNĚNO]
Servisní zásahy a provozní změny
[BUDE DOPLNĚNO]
Dostupnost Cloudových služeb/Služeb KB
[BUDE DOPLNĚNO]
Celkový přehled omezení Cloudových služeb/Služeb KB
[BUDE DOPLNĚNO]
Problémy a rizika
[BUDE DOPLNĚNO]
Zpráva o stavu bezpečnosti
[BUDE DOPLNĚNO]
Smluvní pokuty
[BUDE DOPLNĚNO]
Seznam příloh

P. č.	Název přílohy
1	[BUDE DOPLNĚNO]

Schvalovací doložka

Jméno a příjmení	Organizace	Datum a podpis
[BUDE DOPLNĚNO]	Objednatel	[elektronický podpis včetně data podpisu]
[BUDE DOPLNĚNO]	Poskytovatel	[elektronický podpis včetně data podpisu]

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

NABÍDKA

Identifikační údaje Objednatele	Identifikační údaje Poskytovatele
[BUDE DOPLNĚNO] se sídlem: [BUDE DOPLNĚNO] za niž jedná: [BUDE DOPLNĚNO] IČO: [BUDE DOPLNĚNO] DIČ: [BUDE DOPLNĚNO] Bank. spojení: [BUDE DOPLNĚNO] číslo účtu: [BUDE DOPLNĚNO] ID DS: [BUDE DOPLNĚNO]	**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: Mgr. Jakubem Richterem, 1. zástupcem generálního ředitele IČO: 036 30 919 DIČ: CZ03630919 Bank. spojení: Česká národní banka číslo účtu: 206201/0710 ID DS: ag5uunk

Název a specifikace Služby	[bude doplněno]
Termín zahájení poskytování Služby	[bude doplněno]
Termín ukončení poskytování Služby	[bude doplněno]
Paušální cena za jeden kalendářní měsíc poskytování Cloudové služby/Cloudových služeb/Služby KB/Služeb KB	[bude doplněno v případě Nabídky na Službu dle čl. III odst. 3.3 pododst. 3.3.1 nebo pododst. 3.3.2
Celková cena za nabízené Ostatní činnosti	[bude doplněno v případě Nabídky na Službu dle čl. III odst. 3.3 pododst. 3.3.3 bodu 3.3.3.1

Podrobná specifikace požadované Služby včetně rozsahu	
Popis řešení (vč. uvedení případných poddodavatelů a části Služeb, kterou bude případný poddodavatel poskytovat)	[bude doplněno]
Rizika realizace	[bude doplněno]
Dopady	[bude doplněno]
Bezpečnostní podmínky	[bude odstraněno, nejsou-li požadovány]
Harmonogram plnění Služby	[bude odstraněno, pokud není relevantní v rámci nabízené Služby]
Akceptační kritéria	[bude odstraněno, pokud nejsou relevantní v rámci nabízené Služby]
SLA Služby a smluvní pokuty za nedodržení SLA	[bude odstraněno, pokud nejsou požadována SLA odlišná od SLA stanovených ve Smlouvě pro danou Službu]
Členové realizačního týmu Poskytovatele vč. doložení jejich certifikace, je-li vyžadována	[bude odstraněno, pokud nejsou relevantní v rámci nabízené Služby]
Požadavky na součinnost Objednatele	[bude doplněno]

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Požadavky na součinnost třetích stran	[bude doplněno]

Schvalovací doložka			
Jméno a příjmení	**Smluvní strana**	**Podpis**	**Datum**
[bude doplněno]	Poskytovatel		

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

SPCSS Státní pokladna Centrum sdílených služeb

OBJEDNÁVKA

Ostatní činnosti

číslo **OBJYYYYXXX**

č. j. **SPCSS-xxxxx/20xx**

vystavena dne **[BUDE DOPLNĚNO]**

Objednatel		**Poskytovatel**	
Název	[BUDE DOPLNĚNO]	Název	[BUDE DOPLNĚNO]
Sídlo	[BUDE DOPLNĚNO]	Sídlo	[BUDE DOPLNĚNO]
	[BUDE DOPLNĚNO]		[BUDE DOPLNĚNO]
IČO	[BUDE DOPLNĚNO]	IČO	[BUDE DOPLNĚNO]
DIČ	[BUDE DOPLNĚNO]	DIČ	[BUDE DOPLNĚNO]
Vystavil	[BUDE DOPLNĚNO]	Rámcová smlouva	[BUDE DOPLNĚNO]
Na základě	[BUDE DOPLNĚNO]	Nabídka	[BUDE DOPLNĚNO]
Kontaktní os.	[BUDE DOPLNĚNO]	**Kontaktní os.**	[BUDE DOPLNĚNO]
Telefon	[BUDE DOPLNĚNO]	Telefon	[BUDE DOPLNĚNO]
E-mail	[BUDE DOPLNĚNO]	E-mail	[BUDE DOPLNĚNO]
Název plnění	[BUDE DOPLNĚNO]		

Objednatel objednává od Poskytovatele následující položky:

P. č.	Role	Množství	MJ	Cena za jednotku v Kč bez DPH	Cena celkem v Kč bez DPH
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	ČD	[BUDE DOPLNĚNO]	0,00 Kč
Celkem					**0,00 Kč**

Specifikace Ostatních činností	[BUDE DOPLNĚNO]
Termín dodání	[BUDE DOPLNĚNO]
Místo plnění	[BUDE DOPLNĚNO]
Poznámka	[BUDE DOPLNĚNO]

Za Objednatele		**Za Poskytovatele**	
Jméno, příjmení	[BUDE DOPLNĚNO]	**Jméno, příjmení**	[BUDE DOPLNĚNO]
Datum a podpis		**Datum a podpis**	

Upozorňujeme, že plnit Objednávku lze až po její řádné písemné akceptaci ze strany Poskytovatele s tím, že následně bude potvrzená Objednávka Objednatelem zveřejněna v Registru smluv v souladu s požadavky vyplývajícími ze zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) v platném znění.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

AKCEPTAČNÍ PROTOKOL

Předmět	[BUDE DOPLNĚNO]		
Rámcová smlouva (dále jen „**Rámcová smlouva**“)	[BUDE DOPLNĚNO]		
Objednatel (dále jen „**Objednatel**“)	[BUDE DOPLNĚNO]		
Poskytovatel (dále jen „**Poskytovatel**“)	[BUDE DOPLNĚNO]		
Vypracoval	[BUDE DOPLNĚNO]	**Datum**	[BUDE DOPLNĚNO]

Předmět akceptace
[BUDE DOPLNĚNO]

Připomínky Objednatele
[BUDE DOPLNĚNO]

Závěry akceptace	
☐	je akceptováno bez výhrad
☐	je akceptováno s výhradou
☐	není akceptováno

Seznam výhrad akceptace

P. č.	Popis výhrady	Způsob odstranění	Termín odstranění	Zodpovědná osoba
1	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]

Seznam příloh akceptace

P. č.	Název přílohy
1	[BUDE DOPLNĚNO]
2	[BUDE DOPLNĚNO]

Schvalovací doložka

Jméno a příjmení	Organizace	Datum a podpis
[BUDE DOPLNĚNO]	Objednatel	[elektronický podpis včetně data podpisu]
[BUDE DOPLNĚNO]	Poskytovatel	[elektronický podpis včetně data podpisu]

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

SPCSS Státní pokladna Centrum sdílených služeb

OBJEDNÁVKA

Konzultace

číslo **OBJYYYYXXX**

č. j. **SPCSS-xxxxx/20xx**

vystavena dne **[BUDE DOPLNĚNO]**

Objednatel		**Poskytovatel**	
Název	[BUDE DOPLNĚNO]	Název	[BUDE DOPLNĚNO]
Sídlo	[BUDE DOPLNĚNO]	Sídlo	[BUDE DOPLNĚNO]
	[BUDE DOPLNĚNO]		[BUDE DOPLNĚNO]
IČO	[BUDE DOPLNĚNO]	IČO	[BUDE DOPLNĚNO]
DIČ	[BUDE DOPLNĚNO]	DIČ	[BUDE DOPLNĚNO]
Vystavil	[BUDE DOPLNĚNO]	Rámcová smlouva	[BUDE DOPLNĚNO]
Na základě	[BUDE DOPLNĚNO]	Nabídka	[BUDE DOPLNĚNO]
Kontaktní os.	[BUDE DOPLNĚNO]	**Kontaktní os.**	[BUDE DOPLNĚNO]
Telefon	[BUDE DOPLNĚNO]	Telefon	[BUDE DOPLNĚNO]
E-mail	[BUDE DOPLNĚNO]	E-mail	[BUDE DOPLNĚNO]
Název plnění	[BUDE DOPLNĚNO]		

Objednatel objednává od Poskytovatele následující položky:

P. č.	Role	Množství	MJ	Cena za jednotku v Kč bez DPH	Cena celkem v Kč bez DPH
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	ČH	[BUDE DOPLNĚNO]	0,00 Kč
Celkem					**0,00 Kč**

Specifikace Konzultací	[BUDE DOPLNĚNO]
Doba trvání	[BUDE DOPLNĚNO]
Místo plnění	[BUDE DOPLNĚNO]
Poznámka	[BUDE DOPLNĚNO]

Za Objednatele		**Za Poskytovatele**	
Jméno, příjmení	[BUDE DOPLNĚNO]	**Jméno, příjmení**	[BUDE DOPLNĚNO]
Datum a podpis		**Datum a podpis**	

Upozorňujeme, že plnit Objednávku lze až po její řádné písemné akceptaci ze strany Poskytovatele s tím, že následně bude potvrzená Objednávka Objednatelem zveřejněna v Registru smluv v souladu s požadavky vyplývajícími ze zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) v platném znění.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

VÝKAZ KONZULTACÍ

Období Konzultací	[MĚSÍC/ROK – BUDE DOPLNĚNO]		
Rámcová smlouva (dále jen „**Rámcová smlouva**“)	[BUDE DOPLNĚNO]		
Poskytovatel (dále jen „**Poskytovatel**“)	[BUDE DOPLNĚNO]		
Vypracoval	[BUDE DOPLNĚNO]	**Datum**	[BUDE DOPLNĚNO]

Role	**Popis Konzultací**	**Počet ČH**
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]

Připomínky Objednatele
Připomínky ke Konzultacím

Závěry akceptace	
☐	je akceptováno bez výhrad
☐	je akceptováno s výhradou
☐	není akceptováno

Seznam výhrad akceptace

P. č.	**Popis výhrady**	**Způsob odstranění**	**Termín odstranění**	**Zodpovědná osoba**
1	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]

Seznam příloh Výkazu Konzultací

P. č.	**Název přílohy**
1	[BUDE DOPLNĚNO]

Schvalovací doložka

Jméno a příjmení	**Organizace**	**Datum a podpis**
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[elektronický podpis včetně data podpisu]
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[elektronický podpis včetně data podpisu]

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

ZMĚNOVÝ POŽADAVEK

Číslo Změnového požadavku	[BUDE DOPLNĚNO]		
Název Změnového požadavku	[BUDE DOPLNĚNO]		
Priorita	[BUDE DOPLNĚNO – Nízká / Střední / Vysoká]		
Datum podání	[BUDE DOPLNĚNO]	**Datum aktualizace ZP**	[BUDE DOPLNĚNO]
Rámcová smlouva (dále jen „**Rámcová smlouva**")	[BUDE DOPLNĚNO]		
Objednatel (dále jen „**Objednatel**")	[BUDE DOPLNĚNO]		
Poskytovatel (dále jen „**Poskytovatel**")	[BUDE DOPLNĚNO]		
Předkladatel	[BUDE DOPLNĚNO]		
Zhotovitel	[BUDE DOPLNĚNO]		

ZADÁNÍ
Popis požadované změny
[BUDE DOPLNĚNO]
Dopady na stávající Službu
[BUDE DOPLNĚNO]
Specifikace SW a HW požadavků
[BUDE DOPLNĚNO]
Popis zajištění realizace změny
[BUDE DOPLNĚNO]
Zdůvodnění změny
[BUDE DOPLNĚNO]
Očekávané důsledky
[BUDE DOPLNĚNO]

VÝSLEDEK	
☐	Dále zpracovávat
☐	Nerealizovat
☐	Přepracovat
☐	Odložit

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Schvalovací doložka		
Jméno a příjmení	**Organizace**	**Datum a podpis**
[BUDE DOPLNĚNO]	Manažer Služby Objednatele	[elektronický podpis včetně data podpisu]
[BUDE DOPLNĚNO]	Manažer Služby Poskytovatele	[elektronický podpis včetně data podpisu]

ANALÝZA ZP – TECHNICKÉ ŘEŠENÍ		
Detailní popis řešení		
[BUDE DOPLNĚNO]		
Popis současného stavu		
[BUDE DOPLNĚNO]		
Cílový stav		
[BUDE DOPLNĚNO]		
Realizované činnosti		
[BUDE DOPLNĚNO]		
ID	**Činnost**	**Zodpovědnost**
1	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]
Požadovaná součinnost		
[BUDE DOPLNĚNO]		
Dopady do kvalitativních parametrů poskytované Služby		
[BUDE DOPLNĚNO]		
Harmonogram realizace		
[BUDE DOPLNĚNO]		
Rizika		
[BUDE DOPLNĚNO]		
Cenové ohodnocení pracnosti a nákladů (pokud budou nad rámec Služby)		
[BUDE DOPLNĚNO]		
Dopady do dokumentace		
ID	**Název**	**Popis změny**
1	[BUDE DOPLNĚNO]	aktualizace dokumentu

SPOLEČNÁ SEKCE		
Rozhodnutí		
Datum rozhodnutí	[BUDE DOPLNĚNO]	
Výsledek rozhodnutí	☐	Dále zpracovávat
	☐	Nerealizovat
	☐	Přepracovat
	☐	Odložit

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

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		

SCHVALOVACÍ DOLOŽKA		
Jméno a příjmení	**Organizace**	**Datum a podpis**
[BUDE DOPLNĚNO]	Manažer Služby Objednatele	[elektronický podpis včetně data podpisu]
[BUDE DOPLNĚNO]	Manažer Služby Poskytovatele	[elektronický podpis včetně data podpisu]
[BUDE DOPLNĚNO]	Oprávněná osoba Objednatele	[elektronický podpis včetně data podpisu]
[BUDE DOPLNĚNO]	Oprávněná osoba Poskytovatele	[elektronický podpis včetně data podpisu]

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Rámcová smlouva o poskytování Cloudových a dalších souvisejících služeb

Příloha č. 3 – Odkazy na specifikaci Cloudových služeb a Ceny za Cloudové služby

Odkaz na Katalog Cloudových služeb a Cena za Cloudové služby je uveřejněna na webové adrese:

https://www.spcss.cz/dokumentace/

Pro vyloučení pochybností Smluvní strany uvádějí, že Ceny za Cloudové služby uvedené na webové adrese výše je Poskytovatel oprávněn měnit vždy k prvnímu dni kalendářního čtvrtletí účinnosti Rámcové smlouvy, přičemž o této změně je povinen Objednatele bezodkladně písemně informovat.

Jednotlivé Objednávky budou uzavírány ze ceny uvedené do Nabídky postupem dle Rámcové smlouvy, tj. za ceny platné v daném kalendářním čtvrtletí, ke dni odeslání Nabídky. Ceny uvedené v uzavřené a účinné Objednávce je Poskytovatel oprávněn měnit nejdříve po uplynutí 12 měsíců od účinnosti Objednávky, a to jednostranně formou písemného oznámení Objednateli a současně prostřednictvím změny ceníku zveřejněného na výše uvedené webové adrese, přičemž tato změna je účinná vždy od prvního dne kalendářního měsíce následujícího po měsíci, ve kterém bylo Objednateli doručeno předmětné oznámení. Změna cen prostřednictvím inflační doložky dle Rámcové smlouvy tímto není dotčena.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Rámcová smlouva o poskytování cloudových a dalších souvisejících služeb

Příloha č. 4 – Specifikace Služeb KB – Katalogové listy

Seznam katalogových listů			
Označení	**Název**	**Termíny poskytování Služby**	
		zahájení	**ukončení**
KL_BM	Bezpečnostní monitoring	V souladu s konkrétní Objednávkou	V souladu s konkrétní Objednávkou
KL_PU	Správa privilegovaných účtů		
KL_VM	Vulnerability management		
KL_KC	Kompetenční centrum kybernetické bezpečnosti		

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

KATALOGOVÝ LIST – BEZPEČNOSTNÍ MONITORING

Název služby	**Bezpečnostní monitoring**

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Bezpečnostní monitoring (dále jen **„Služba KL_BM"**) je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL_BM.

Název milníku	**Termín splnění milníku**
Zahájení poskytování Služby KL_BM	Na základě Objednávky/Smlouvy
Ukončení poskytování Služby KL_BM	Na základě Objednávky/Smlouvy

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba KL_BM bude poskytována v režimu, dle popisu v tabulce:

Režim poskytování Služby KL_BM	**Doba poskytování Služby KL_BM**
Standardní provozní doba	Nepřetržitě (24x7)

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 Vstupy

Vstupy pro Službu KL_BM jsou:

- Relevantní dokumenty Objednatele;
- Vstupní analýza – zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování odpovídajícího plnění;
- Realizace ověření provozu – zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování plnění.

3.2 Výstupy

Výstupy Služby KL_BM jsou:

- Poskytování Služby KL_BM;

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

- měsíční zpráva o stavu služby dle tohoto katalogového listu;
- dokumentace Nasazení Služby Bezpečnostního monitoringu v rozsahu Objednávky Objednatele
- a Proces zvládání kybernetických bezpečnostních incidentů.

4 POPIS ROZSAHU SLUŽBY

Služba KL_BM 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 KL_BM je poskytována v nepřetržitém režimu 24x7 a zahrnuje sběr informací, jejich třídění, korelaci, kategorizaci, analýzu a archivaci. Použité technologie a nástroje umožňují detekci známých bezpečnostních útoků, podezřelého chování a anomálií. V rámci Služby KL_BM je také poskytován incident management 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 KL_BM je rozdělena do čtyř částí. Část 1 je určena k zajištění povinností stanovených příslušnou legislativou, blíže popsáno v kapitole 4.1. Část 2 doplňuje funkcionalitu Služby KL_BM, nedostupnost jednotlivých součástí Části 2 nemá vliv na poskytování služby v rozsahu Části 1, tedy na zajištění povinností stanovených příslušnou legislativou. Část 1 a Část 2 jsou nedílné součásti Služby KL_BM.

V Části 3 a 4 jsou obsaženy Doplňkové služby, které jsou nezbytné k zajištění poskytování služby, a to dle požadované architektury, která je určena na základě Vstupní analýzy dle kapitoly 3.1. Doplňkové služby v této části mohou mít vliv na poskytování služby v rozsahu Části 1, tedy na zajištění povinností stanovených příslušnou legislativou.

Část 1 - Součásti služby Bezpečnostní monitoring povinné k naplnění vybraných opatření (nedílné součásti KL_BM, poskytováno vždy)	
☒	Sběr logů
☒	Zpracování logů
☒	Monitorování NetFlow
☒	Proces zvládání kybernetických bezpečnostních incidentů (Incident management)
Část 2 - Ostatní součásti služby Bezpečnostní monitoring (nedílné součásti KL_BM, poskytováno vždy)	
☒	Uživatelská behaviorální analýza
☒	Přístup do prostředí nástroje SIEM v rozsahu Služby KL_BM
☒	Zpracování zprávy o stavu Služby KL_BM dle tohoto katalogového listu určené Objednateli (předávána v měsíčním intervalu)
Část 3 - Doplňkové služby – Bezpečnostní monitoring databází	
☐	Bezpečnostní monitoring databází
☐	Virtuální kolektor pro Bezpečnostní monitoring databází
☐	Virtuální agregátor pro Bezpečnostní monitoring databází

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

☐	Virtualizace pro provozování Doplňkových služeb v prostředí SPCSS
☐	Úložný prostor
Část 4 - Doplňkové služby – Bezpečnostní monitoring	
☐	Virtuální kolektor pro Bezpečnostní monitoring
☐	Virtuální procesor pro Bezpečnostní monitoring
☐	Virtualizační prostředí pro provozování služby v prostředí SPCSS
☐	Úložný prostor

Služba KL_BM je realizována v rozsahu definovaných aktiv Objednatele. Archivované informace slouží pro forenzní analýzu ve všech sledovaných souvislostech.

V rámci Služby KL_BM je poskytován proces zvládání kybernetických bezpečnostních incidentů (incident management), včetně přípravy podkladů pro hlášení příslušným orgánům. Shromažďované informace jsou na základě požadavku předány pro potřebu interního vyšetřování nebo pro potřeby orgánů činných v trestním řízení.

4.1 Plnění legislativních povinností Objednatele

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. KL_BM obsahuje obecný výčet rozsahu bezpečnostních opatření, které poskytuje Objednateli. Specifika dle klasifikace informací a povahy spravovaného systému (jako KII, VIS) jsou ze strany Objednatele určeny Objednávkou, specifikovány Vstupy dle kapitoly 3.1 a budou zaznamenány v dokumentu „Nasazení Služby Bezpečnostního monitoringu v rozsahu Objednávky Objednatele a Proces zvládání kybernetických bezpečnostních incidentů" dle kapitoly 3.2.

Jedná se o tato opatření:

§ 14 Zvládání kybernetických bezpečnostních událostí a incidentů

Služba KL_BM zahrnuje procesy pro detekci a vyhodnocování kybernetických bezpečnostních událostí, zvládání kybernetických bezpečnostních incidentů, ohlašování a posuzování. Služba nabízí nástroje pro klasifikaci, prošetření bezpečnostních událostí včetně návrhu opatření pro odvracení a zmírňování škod.

§ 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

Služba Bezpečnostní monitoring zaznamenává bezpečnostní logy včetně bezpečného uchovávání po dobu požadovanou VoKB (Podmínkou pro splnění tohoto opatření je realizace samostatné Služby Log management SPCSS, která není předmětem tohoto KL_BM, nebo využití odpovídajících Doplňkových služeb specifikovaných na základě Vstupní analýzy dle kapitoly 3.1).

§ 23 Detekce kybernetických bezpečnostních událostí

Služba KL_BM disponuje nástroji pro detekci kybernetických bezpečnostních událostí, ověřováním a kontrolou přenášených dat v komunikačních sítí a na jejím perimetru.

Při ochraně prostředí Objednatele umožňuje s ohledem na důležitost aktiv zajistit detekci kybernetických bezpečnostních událostí v rámci koncových stanic, mobilních zařízení, serverů, datových úložišť a výměnných datových nosičů, síťových aktivních prvků a obdobných aktiv.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

§ 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí

V prostředí Objednatele lze Službu KL_BM využít pro sběr bezpečnostních událostí a jejich vyhodnocování. Služba KL_BM poskytuje informace určeným bezpečnostním rolím v organizaci, čímž omezuje případy nesprávného vyhodnocení události a zajišťuje včasné varování.

§ 31 Kategorizace kybernetických bezpečnostních incidentů

Služba KL_BM umožňuje kategorizovat jednotlivé bezpečnostní incidenty dle významnosti. Bezpečnostní incidenty lze kategorizovat dle dopadových kritérií, počtu dotčených uživatelů, škod způsobených nebo předpokládaných. Kategorizovat lze také podle dopadu na služby nebo délkou trvání incidentu.

§ 32 Forma a náležitosti hlášení kybernetických bezpečnostních incidentů

Služba Bezpečností monitoring zajišťuje přípravu podkladů, vytvoření hlášení o kybernetickém bezpečnostním incidentu. Po zajištění všech potřebných informací provede nahlášení patřičným způsobem a formou příslušným orgánům.

Služba KL_BM nezahrnuje organizační opatření SŘBI Objednatele. Součástí Služby KL_BM není tvorba politik, vyjma dokumentace dle kapitoly 3 tohoto katalogového listu.

5 POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL_BM

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

Typy záznamů, se kterými Služba KL_BM pracuje, jsou zejména:

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

5.1 Zpracování logů

Služba je poskytována za využití nástrojů a prostředků ve vlastnictví SPCSS, které zprostředkovávají realizaci sběru, vyhodnocování a uchovávání logů.

Zpracování logů má významnou funkci nejen pro analýzu obsažených informací, ale i pro ochranu před ztrátou, poškozením nebo úmyslnou modifikací těchto záznamů. Ze systémových logů lze čerpat celou řadu informací, např.: přihlášení uživatele, informace o uživatelských aktivitách, záznam o konfiguračních změnách systému a jiné. Získané informace lze využít k detekci anomálií chování uživatelů, infrastruktury nebo samotných aplikací.

Dalším opatřením, které stanovuje VoKB je ukládání získaných informací – logů, v bezpečném úložišti, které zajišťuje ochranu proti změnám nebo smazání. Logy získané z monitorovaných aktiv Objednatele je nezbytné uchovávat po dobu stanovenou VoKB pro příslušný typ systému. Uchování logů není součástí služby KL_BM. Podmínkou pro splnění tohoto opatření je realizace samostatné Služby Log management SPCSS, která není předmětem tohoto KL_BM nebo dle dohody mezi smluvními stranami.

5.2 Monitorování NetFlow

Tato služba obsahuje monitorování síťového provozu na základě datových toků na síťové vrstvě. Tento způsob monitorování poskytuje podrobný pohled do provozu na síti v reálném čase. S pomocí NetFlow statistik lze odhalovat vnější i vnitřní incidenty, sledovat zdroje a cíle komunikace, jak dlouho, pomocí jakého protokolu a kolik bylo přeneseno dat. Monitorování NetFlow důrazně doporučujeme s ohledem na

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

kontext vyhodnocování událostí z monitorovaných systémů. Informace o NetFlow výrazně zvýší přehled o dění v monitorovaných systémech a dokáže odhalit například podezřele dlouhé, nebo objemné přenosy dat nejen do internetu, ale i v rámci infrastruktury Objednatele nebo komunikaci s IP adresami s nízkou reputací (rozesílání, malware, spamu, skenování atd.). Pro monitoring NetFlow v prostředí Objednatele je doporučena instalace NetFlow kolektoru (jedná se o službu Virtuální kolektor pro bezpečnostní monitoring) z důvodu úspory kapacity datového toku a zaručení dodávky dat do SIEM.

Integrace, konfigurace a správa NetFlow kolektoru není součástí základní Služby KL_BM.

Dodávka NetFlow kolektoru je řešena jako doplňková služba Virtuální kolektor pro bezpečnostní monitoring. Doporučení pro využití NetFlow kolektoru (Virtuální kolektor pro bezpečnostní monitoring) je stanoveno na základě Vstupní analýzy dle kapitoly 3.1.

5.3 Uživatelská behaviorální analýza

Služba obsahuje analýzu chování uživatelů (User behavior analytics – UBA). Technologie analyzuje aktivitu uživatelů a zjišťuje, zda došlo ke zneužití účtu uživatele. UBA přidává kontext uživatele k síti, protokolu, zranitelnostem a ohrožení dat rychleji a přesněji detekuje útoky. Bezpečnostní analytici mohou snadno zobrazit rizikové uživatele, zobrazit jejich anomální aktivity a zkoumat konkrétní podkladové protokoly, logy a toky dat, která přispěla k hodnocení rizika uživatele.

5.4 Přístup do prostředí nástroje SIEM v rozsahu Služby KL_BM

V rámci služby je určeným pracovníkům Objednatele umožněn přístup do prostředí SIEM, kde mohou sledovat aktivity, které generují monitorované systémy. Objednatel si může nastavit vlastní přehledové obrazovky a grafy, sledovat Offense nebo výpisy z logů, které jsou zpracovány nástrojem SIEM. Objednatel má přístup pouze k informacím v rozsahu svých systémů.

Prostředí zpřístupněné Objednateli (tzv. tenant) je vyhrazené prostředí, které vidí pouze daný Objednatel. Data jsou zpracovávána a ukládána v daném prostředí tenanta.

Toto prostředí slouží pouze jako přehledové s možností dohledávání historických dat. Náhled neslouží pro vyšetřování KBU, KBI ani pro analýzy.

Při nasazení služby proběhne školení určených pracovníků Objednatele. Toto školení bude realizováno dle požadavku Objednatele, nejméně jednou za rok.

Maximální počet pracovníků Objednatele, kteří budou moci využívat přístup do prostředí SIEM, je stanoven na 10 pracovníků.

Nedostupnost tohoto prostředí Objednateli nemá vliv na řešení KBU/KBI ze strany Poskytovatele, neovlivňuje dostupnost a kvalitu poskytované služby bezpečnostního monitoringu a nemá tak vliv na plnění SLA; více v kapitole 6 tohoto katalogového listu.

5.5 Incident management – proces zvládání kybernetických bezpečnostních incidentů

Incident response je aplikován na zvládání všech zjištěných nebo hlášených událostí a incidentů. Expertní týmy aktivně řeší události od počátku až po jeho vyřešení a uzavření. Aktivita týmů zahrnuje vyhodnocování, zvládání, dokumentování Bezpečnostních Hlášení (BH), Kybernetických Bezpečnostních událostí (KBU) a Kybernetických Bezpečnostních incidentů (KBI). Nedílnou součástí je analýza a návrh na zlepšování bezpečnosti Informačních Systémů (IS) ve sledovaném prostředí. Primárním subjektem odpovědným za řešení a zvládání událostí a incidentů je CSIRT–SPCSS.

Monitoring a detekce KBU a KBI v režimu 24x7 je zajištěna dohledovým pracovištěm SPCSS, nástrojem SIEM a expertním týmem Security Operation Center (dále také jen „SOC“). Nástroj SIEM v reálném čas monitoruje a vyhodnocuje probíhající události na sledovaných aktivech a na základě implementovaných pravidel automaticky sestavuje bezpečnostní výstrahy, které nesou informace o narušení bezpečnostního stavu. Tato funkcionalita je zajištěna sběrem událostí v nástroji SIEM z vybraných zdrojů logů, které jsou definovány na základě podkladů od Objednatele, resp. na základě analýzy rizik.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Řízení incidentů je vedeno pomocí systému podchycujícího jednotlivé kroky odborníků, vyšetřujících detekované nebo hlášené události (Incident Response Platform). Tento nástroj pomáhá od počátku až do finálního vyřešení požadavku. Velký význam nástroje je v jeho specifické funkcionalitě, která agreguje bezpečnostní informace z rozdílných zdrojů na jednom místě. Toto propojení informací na jednom místě pomáhá při řešení sofistikovaných útoků, jejichž počet v poslední době narůstá. Jedním ze zdrojů je otevřená platforma pro sdílení informací o hrozbách, které jsou aktualizovány v celosvětovém měřítku (Threat Intelligence Platform).

Nezbytným pro činnost CSIRT-SPCSS při provádění evidence a vyhodnocování událostí je aplikace Service Desk. Jedná se o jednotné prostředí pro řízení procesu Incident response. V aplikaci je prováděna evidence stavu i jednotlivé kroky řešení události. Systém umožňuje sledovat průběh události, ale i následné řešení. Podklady zpracovávané v systému Service Desk slouží k řešení a vyhodnocování bezpečnostních hlášení, kybernetických bezpečnostních událostí nebo kybernetických bezpečnostních incidentů. Zdroje pro vyhodnocované události mohou pocházet od uživatelů, bezpečnostních specialistů, administrátorů nebo pomocí technických prostředků.

Service Desk je prostředí obsahující informace, které slouží jako podklad pro expertní tým OCKB – SOC při zvládání kybernetických bezpečnostních událostí a bezpečnostních incidentů. Definovanými procesy v prostředí Service Desk jsou uzpůsobeny pro zvládání KBU a KBI a následné řízení změn.

Aktivity CSIRT-SPCSS poskytované v rámci služby pro zvládání kybernetických bezpečnostních incidentů:

- zabezpečení procesu zvládání BH, KBU, KBI;
- detekci KBU, KBI;
- klasifikaci KBU, KBI;
- zpracování dokumentace KBU a KBI včetně uchovávání relevantních dat v nástroji SIEM (logů, událostí, „offense"…), vedení záznamů v Service Desk (systém zákaznické podpory, dále jen SD) o průběhu řešení, zavedení a aktualizace znalostní báze v SD;
- iniciaci bezpečnostních varování a opatření včasné reakce v případech velmi závažných a závažných KBI;
- zajištění realizace reaktivních opatření NÚKIB;
- příprava proaktivních opatření obrany v závislosti na rozvoj hrozeb;
- přípravu podkladů pro informování příslušných orgánů.

5.6 Pravidelná zpráva o stavu služby dle tohoto katalogového listu

Zpráva obsahuje tyto informace:

- Období poskytování Služby KL_BM;
- Režim poskytování Služby KL_BM;
- Popis rozsahu Služby KL_BM;
- Monitorovaná prostředí;
- Rozsah bezpečnostního dohledu;
- Detekce, sběr a vyhodnocování kybernetických bezpečnostních událostí;
- Stav dokumentace (aktualizace dokumentace dle kapitoly 3.2);
- Řešení a stav BH (Bezpečnostní hlášení), KBU, KBI za uplynulé období a návrhy na nápravná opatření;
- Aktivity Služeb Bezpečnostního dohledu – seznam řešených offense;

- Návrh na nápravná opatření.

6 SLA PARAMETRY

Poskytovatel je povinen poskytovat Službu KL_BM dle Smlouvy pro vybrané aktiva Objednatele v souladu s jednotlivými níže uvedenými kvalitativními parametry Služby pro její jednotlivé části.

Ovlivnění chodu všech částí Služby KL_BM ze strany Objednatele (přerušení zasílání logů úplné nebo částečné a obdobné) a z důvodů mimo působnost Poskytovatele se nezapočítává do nedostupnosti žádné z částí Služby KL_BM.

6.1 Požadovaná měsíční dostupnost částí služby – VYBRANÁ ČÁST ČÁSTI 1, ČÁST 3 a ČÁST 4

Název Služby:	**Bezpečnostní monitoring**	
SLA parametry		
Část Služby:	Dostupnost Služby:	Servisní okno pro odstávky:
Část 1 - Sběr logů, zpracování logů, Monitoring Netflow v nástroji SIEM	99,5 %	každý čtvrtek, vždy 19:00-24:00
Část 3 - Bezpečnostní monitoring databází, Virtuální kolektor pro Bezpečnostní monitoring databází, Virtuální agregátor pro Bezpečnostní monitoring databází	99,5 %	každý čtvrtek, vždy 19:00-24:00
Část 4 - Virtuální kolektor pro Bezpečnostní monitoring, Virtuální procesor pro Bezpečnostní monitoring,	99,5 %	každý čtvrtek, vždy 19:00-24:00

Tabulka – Požadovaná měsíční dostupnost částí služby – vybraná část Části 1, Část 3 a Část 4

Nedostupnost Služby KL_BM – Část 1 (Sběr logů, zpracování logů, Monitoring Netflow v nástroji SIEM), Část 3 (Bezpečnostní monitoring databází, Virtuální kolektor pro Bezpečnostní monitoring databází, Virtuální agregátor pro Bezpečnostní monitoring databází) Část 4 (Virtuální kolektor pro Bezpečnostní monitoring, Virtuální procesor pro Bezpečnostní monitoring,) způsobená hardwarovou nebo jinou technickou závadou se počítá od okamžiku zahájení nedostupnosti Služby KL_BM – Část 1, Část 3 a Část 4 ve výše definovaném rozsahu do okamžiku obnovení poskytování. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti Služby KL_BM – Část 1, Část 3 a Část 4 ve výše definovaném rozsahu, počítá se nedostupnost služby od doby jejího nahlášení.

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

Nedostupnost součástí Služby KL_BM – Část 2 - Uživatelská behaviorální analýza, Přístup do prostředí nástroje SIEM v rozsahu Služby KL_BM, Zpracování zprávy o stavu Služby KL_BM dle tohoto katalogového listu určené Objednateli (předávána v měsíčním intervalu) - neovlivňuje dostupnost a kvalitu poskytované Služby KL_BM – Část 1, Část 3 a Část 4 ve výše definovaném rozsahu a nemá tak vliv na plnění příslušného SLA.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

6.1.1 Postup výpočtu dostupnosti Služby

Dostupnost služby se vypočítá podle následujícího vzorce:

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

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, mimořádné odstávky a další specifické Části Služby KL_BM.

6.1.2 Požadované lhůty pro obnovení Služby KL_BM – Vybraná část Části 1, Část 3 a Část 4

Název Služby:	**Bezpečnostní monitoring**		
Část Služby:	**Lhůta pro obnovení služby v běžné provozní době v hodinách**		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Část 1 – Sběr logů, zpracování logů, Monitoring Netflow v nástroji SIEM	6	24	168
Část 3 - Bezpečnostní monitoring databází, Virtuální kolektor pro Bezpečnostní monitoring databází, Virtuální agregátor pro Bezpečnostní monitoring databází	6	24	168
Část 4 - Virtuální kolektor pro Bezpečnostní monitoring, Virtuální procesor pro Bezpečnostní monitoring	6	24	168

Tabulka – Požadované lhůty pro obnovení Služby KL_BM – vybraná část Části 1, Část 3 a Část 4

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Kategorizace provozních incidentů:	
Incident kategorie A	Služba není dostupná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje její užívání. Tento stav kritickým způsobem omezuje běžný provoz.
Incident kategorie B	Služba je ve svých funkcích degradována tak, že tento stav zásadně omezuje (Nefunkční dílčí součást v rozsahu vybrané součásti Části 1 a Část 3) její běžný provoz.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

Tabulka – Kategorizace provozních incidentů

6.2 Reakční doby a doby odstranění kybernetického bezpečnostního incidentu Služby KL_BM – Část 1

Doba reakce úrovně L1 je počítána od zaevidování offense/bezpečnostního hlášení/kybernetické bezpečnostní události/kybernetického bezpečnostního incidentu (BH/KBU/KBI) do aplikace Service Desk SPCSS (servicedesk.spcss.cz). Podpora L1 musí do doby uvedené v tabulce níže přijmout v aplikaci Service Desk BH/KBU/KBI k řešení.

Název Služby:	**Bezpečnostní monitoring**		
Část Služby:	**Maximální doba zahájení řešení incidentu v pracovní dny 6–18 hod.**	**Maximální doba zahájení řešení incidentu v mimopracovní dny a v době 18–6 hod.**	**Doba odstranění incidentu**
Část 1 – Proces zvládání kybernetických bezpečnostních incidentů (Incident management)	15 minut	30 minut	Po dohodě obou smluvních stran

Tabulka – Reakční doby a doby odstranění incidentu

6.3 Požadovaná měsíční dostupnost části služby – Část 2 - Přístup do prostředí nástroje SIEM v rozsahu Služby KL_BM

Název Služby:	**Bezpečnostní monitoring**	
SLA parametry		
Část Služby:	Dostupnost Služby:	Servisní okno pro odstávky:

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Název Služby:	Bezpečnostní monitoring	
SLA parametry		
Část 2 – Přístup do prostředí nástroje SIEM v rozsahu Služby KL_BM	95 %	každý čtvrtek, vždy 19:00-24:00

Tabulka – Přístup do prostředí nástroje SIEM v rozsahu Služby KL_BM

Nedostupnost Služby KL_BM – Část 2 (Přístup do prostředí nástroje SIEM v rozsahu Služby KL_BM) způsobená hardwarovou nebo jinou technickou závadou se počítá od okamžiku zahájení nedostupnosti Služby KL_BM – Část 2 ve výše definovaném rozsahu do okamžiku obnovení poskytování. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti Služby KL_BM – Část 2 ve výše definovaném rozsahu, počítá se nedostupnost služby od doby jejího nahlášení.

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

Lhůta pro obnovení služby v běžné provozní době v hodinách je stanovena dle incidentu Kategorie C dle kapitoly 6.1.2 tohoto Katalogového listu.

Ovlivnění chodu částí Služby KL_BM Část 2 – Přístup do prostředí nástroje SIEM v rozsahu Služby KL_BM ze strany Objednatele (přerušení komunikace na straně Objednatele, a to úplné nebo částečné a obdobné) se nezapočítává do nedostupnosti žádné z částí Služby KL_BM Část 2 – Přístup do prostředí nástroje SIEM v rozsahu Služby KL_BM.

6.4 Plánované odstávky

V rámci poskytování Služby KL_BM si Poskytovatel vyhrazuje právo na plánované odstávky celého nebo částí systému z důvodu údržby jak samotného systému, tak infrastruktury a datové konektivity Poskytovatele. Poskytovatel se zavazuje plánované práce s vlivem na dostupnost Služby KL_BM soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL_BM ovlivněna co nejméně.

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

7 DOPLŇKOVÉ SLUŽBY

Doplňkové služby nemohou být poskytovány samostatně. Podmínkou pro poskytování doplňkových služeb je využití hlavní služby Bezpečnostní monitoring, respektive službu Bezpečnostní monitoring databází, dle povahy řešení. Režim poskytování doplňkových služeb je v souladu s kapitolou 2 a kapitolou 6 tohoto katalogového listu.

7.1 Bezpečnostní monitoring databází

Doplňková služba Bezpečnostní monitoring databází pomáhá se zabezpečením citlivých dat v prostředí databází a datových skladů. Bezpečnostní monitoring databází se skládá ze dvou částí – kolektor (jedná se o kolektor speciálně určený pro monitoring databází) a nástroj pro analýzu a ochranu dat v databázích. Pro integraci služby je zapotřebí využít obě položky.

Systém umožňuje chránit strukturovaná i nestrukturovaná data. Monitoruje a vyhodnocuje činnosti uživatelů databáze a databázových administrátorů. Služba umožňuje chránit data s ohledem na platná

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

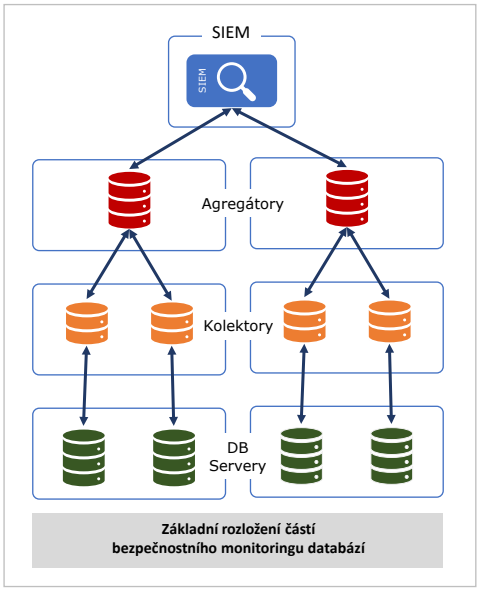
pravidla a nařízení, nabízí kontrolu nad tím, jak je s informacemi zacházeno. Služba pomáhá v pokrytí požadavků v oblastech definovaných legislativou. Rozsah funkcionalit služby se pohybuje v rozsahu od obecných hrozeb až po nesplnění náplně regulačních auditů. Architektura služby je škálovatelná. Služba se skládá vždy ze dvou položek: systému pro obranu databází a kolektoru. Kolektor agreguje a zpracovává data až ze šesti databázových serverů.

Služba dokáže porozumět všem transakcím, ve všech protokolech, na celé řadě platforem. Služba pomáhá v situacích, kdy se rozsah dat mění dynamicky a data jsou distribuovaná v různých místech.

V takto komplexních situacích je využití běžných logovacích mechanismů, které jsou součástí vlastních systémů, velmi komplikované a nedostatečné. Běžné logovací mechanismy také nemají nástroje pro zajištění důvěrnosti logovaných informací. Výsledkem využití služby monitoringu databází je komplexní pohled na informace o využívání dat, přehled chování uživatelů a kontrola pravidel přístupu k informacím v celkovém kontextu sledovaného systému.

Pokud se jedná o neautorizované změny informací z uživatelských účtů, dokáže systém identifikovat autora změn. Informace o aktivitách uživatelů jsou vytvářeny nezávisle na logovacích a auditních funkcích databáze jako takové. Pomocí služby lze sledovat i vynucovat bezpečnostní pravidla pro přístup k citlivým datům (informace typu PII, PCI atd.).

Pro testování ohrožení a zjišťování rizik využívá služba automatizované klasifikační techniky nové generace na bázi kognitivní analýzy. Služba využívá informace, které získává analýzou z pravidelného chování uživatele, a je tak schopna zabránit aktivitám, které nejsou popsány pravidly – např. může se jednat o skenování a vytěžování dat v případě pokusu o odcizení. Systém je schopen v reálném čase detekovat, předávat notifikace, ale i ochránit data.



Služba je schopna generovat výstupy pro potřeby auditu z celé sledované oblasti. Zajištěná auditní stopa, kterou služba poskytne, je chráněna proti nedovolené manipulaci a obsahuje informace požadované auditory.

Pomocí služby Bezpečnostní monitoring databází lze monitorovat a chránit databáze a datové sklady provozované na Windows, UNIX, Linux, AS/400.

Doporučení pro využití služby Bezpečnostního monitoringu databází v rámci architektury řešení poskytované Služby KL_BM je stanoveno na základě Vstupní analýzy dle kapitoly 3.1.

7.2 Virtuální kolektor pro Bezpečnostní monitoring databází

Doplňková služba Virtuální kolektor je nedílnou součástí při využití Bezpečnostního monitoringu databází. Kolektor provádí nasazení zásad ochrany informací, provádí procesy auditu. Dále sbírá, analyzuje, a loguje aktivity databází v reálném čase. Služby virtuálního kolektoru slouží pro okamžité zasílání alertů, ale i pro následnou analýzu. Tento kolektor umí zpracovávat informace z více databázových serverů. Počet napojených serverů, je závislý na celé řadě parametrů, jejichž prověření je předmětem Vstupní analýzy. Dle rozsahu infrastruktury je možné implementovat více kolektorů pro Bezpečnostní monitoring databází. Virtuální kolektor pro bezpečnostní monitoring databází lze provozovat v režimu vysoké dostupnosti. Kolektor je umísťován co nejblíže zdroji/databázím v prostředí Objednatele (virtualizace). Výrobcem je definován maximální počet databázových serverů, které lze připojit na jeden kolektor.

Požadovaný rozsah zdrojů virtualizace (vCPU, vRAM, HDD) je specifikován na základě Vstupní analýzy dle kapitoly 3.1.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Doporučení pro využití Virtuálního kolektoru databází v rámci architektury řešení poskytované Služby KL_BM je stanoveno na základě Vstupní analýzy dle kapitoly 3.1.

7.3 Virtuální agregátor pro Bezpečnostní monitoring databází

Doplňková služba Virtuální agregátor konsoliduje data z kolektorů a zároveň poskytuje možnosti uchovávání a správu dat. Toto řešení je primárně určeno pro centrální správu všech instancí Bezpečnostního monitoringu databází, které jsou na něj připojeny.

Virtuální agregátor je umísťován co nejblíže zdroji informací v prostředí Objednatele nebo v prostředí SPCSS NDC, a to v případě, že je definované aktivum Objednatele provozováno v prostředí NDC. Výrobcem je definován maximální počet kolektorů, které lze připojit na jeden agregátor.

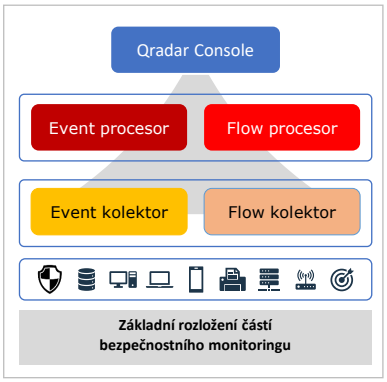
Požadovaný rozsah zdrojů virtualizace (vCPU, vRAM, HDD) je specifikován na základě Vstupní analýzy dle kapitoly 3.1.

Pokud je implementován Virtuální agregátor v prostředí SPCSS NDC, je cena za poskytované prostředky virtualizace (vCPU, vRAM, HDD – Doplňkové služby Virtualizace pro provozování Doplňkových služeb v prostředí SPCSS, Úložný prostor) kalkulována samostatně. Rozsah potřebných prostředků je závislý na velikosti monitorovaného prostředí.

Doporučení pro využití a umístění Virtuálního agregátoru databází v rámci architektury řešení poskytované Služby KL_BM je stanoveno na základě Vstupní analýzy dle kapitoly 3.1.

7.4 Virtuální kolektor pro Bezpečnostní monitoring

Nejedná se o doplněk ke službě Bezpečnostní monitoring databází, služba Bezpečnostní monitoring databází má vlastní kolektor.



Doplňková služba Virtuální kolektor pro bezpečnostní monitoring je určena pro monitorované aktivum Objednatele, které je z pohledu architektury sítě mimo prostředí SPCSS. Kolektor je umístěn do síťového prostředí, kde se nachází monitorovaný systém. Tento kolektor je appliance umístěná ve virtualizačním prostředí. Kolektor slouží k zabezpečenému (šifrovanému) a zaručenému (potvrzovanému) přenosu logů do nástroje SIEM, a to i v případě, že je spojení mezi kolektorem a nástrojem SIEM přerušeno. V době přerušení spojení kolektor ukládá logy do mezipaměti. V okamžiku obnovení spojení se logy z mezipaměti odešlou do nástroje SIEM. Kolektor má tři módy odesílání logů:

- Odesílání logů v reálném čase;
- Odesílání logů dávkově;
- Řízení šířky pásma při odesílání logů.

Virtuální kolektor je umísťován co nejblíže zdroji informací v prostředí Objednatele (virtualizace).

Požadovaný rozsah zdrojů virtualizace (vCPU, vRAM, HDD) je specifikován na základě Vstupní analýzy dle kapitoly 3.1.

Doporučení pro využití a umístění Virtuálního kolektoru pro bezpečnostní monitoring v rámci architektury řešení poskytované Služby KL_BM je stanoveno na základě Vstupní analýzy dle kapitoly 3.1.

7.5 Virtuální procesor pro Bezpečnostní monitoring

Doplňková služba Virtuální procesor zpracovává a analyzuje události, které získává z jednoho nebo více kolektorů. Každý procesor má lokální úložiště, data událostí jsou tedy uložena v procesoru, ale je možné

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

data ukládat i mimo do datového nodu. Virtuální procesor pro bezpečnostní monitoring může být implementován jak v prostředí Objednatele, tak v prostředí SPCSS NDC.

Požadovaný rozsah zdrojů virtualizace (vCPU, vRAM, HDD) je specifikován na základě Vstupní analýzy dle kapitoly 3.1.

Pokud je implementován Virtuální procesor pro bezpečnostní monitoring v prostředí SPCSS NDC, je cena za poskytované prostředky virtualizace (vCPU, vRAM, HDD – Doplňkové služby Virtualizace pro provozování Doplňkových služeb v prostředí SPCSS, Úložný prostor) kalkulována samostatně. Rozsah potřebných prostředků je závislý na velikosti monitorovaného prostředí.

Doporučení pro využití a umístění Virtuálního procesoru v rámci architektury řešení poskytované Služby KL_BM je stanoveno na základě Vstupní analýzy dle kapitoly 3.1.

7.6 Virtualizační prostředí pro provozování služby v prostředí SPCSS

Doplňková služba slouží k zajištění a provozování virtualizovaného prostředí Služby KL02 v případě realizace v prostředí SPCSS NDC.

Požadovaný rozsah zdrojů virtualizace je specifikován na základě Vstupní analýzy dle kapitoly 3.1.

Standardem je platforma x86, 64bit. Virtualizační platforma je provozována na technologii VMware v minimální verzi VMware vSphere 6.7. Součástí služby jsou SW licence virtualizační platformy a aktualizace verzí virtualizačního SW. Na úrovni virtualizace jsou fyzické core mapovány na virtuální CPU (vCPU). Poměr agregace vCPU 10:1 core a zajištění alokace výkonu 1 vCPU odpovídajícího výkonu 1 fyzického core je realizováno prostředky VMware a je v odpovědnosti Dodavatele. Mapování RAM: vRAM je 1:1.

Prostředí se skládá z těchto jednotek:

7.6.1 Building block

Základní stavební jednotkou je Building block (dále také „BB"). Pro provoz virtuálních systémů UNIX/Linux je stanoven BB s poměrem 1:2 (1 vCPU + 2 GB vRAM).

7.6.2 UNIX / LINUX/Linux Critical, Unix-Linux High

Správa operačních systémů různých typů (Unix, Linux) včetně využití externí L3 podpory operačních systémů.

- Dostupnost (roční): 99,9 % pro OS umístěné na replikovaných BB. 99,5 % pro OS umístěné na nereplikovaných BB
- Provozní doba: 24x7 pro Critical, 11x5 pro High

Jednotka obsahuje správu operačních systémů na úrovni fyzických i virtuálních serverů. Administrátorské účty OS jsou v rukou Dodavatele. Objednatel používá pro implementaci a podporu provozu aplikací uživatelské účty, využití administrátorských účtů je možné pouze se součinností Dodavatele nebo bezpečným mechanismem schváleným Dodavatelem.

Služba zahrnuje následující činnosti:

- 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);

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

- Profylaxe systému dle harmonogramu v měsíčních intervalech;
- Součinnosti s případnou instalací a konfigurací nového software;
- Instalace a údržba ovladačů a firmware hardwaru;
- 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 naplněnost);
- Komunikace a řešení problémů s externí L3 podporou;

Předpokladem poskytování služeb je splnění následujících pravidel:

- Účty s administrátorskými právy jsou v rukách Dodavatele. Použité vyšších práv uživatelským nebo aplikačním účtům Objednatele probíhá formou nástrojů typu sudo nebo pod dohledem pracovníků Dodavatele a ve všech případech podléhá schválení ze strany Dodavatele;
- Aplikační adresáře s rostoucím objeme dat (logy, databáze, úložiště souborů) jsou umístěny na samostatných diskových prostorech (volume, logický disk);

7.6.3 Replikované jednotky

Replikované varianty jednotek zajišťují vysokou dostupnost prostředky virtualizační platformy. Ke každému BB je alokován záložní BB ve druhém DC. V případě výpadku zdrojů v jednom DC dojde k obnovení provozu v druhém DC. Replikace se provádí na úrovni virtuálních serverů (tj. všechny BB jednoho virtuálního serveru musí být replikované) a předpokladem je rovněž zdvojená konfigurace všech diskových prostorů STOR1 nebo STOR3 daného virtuálního serveru. Replikace diskových prostorů do druhého DC se provádí prostředky virtualizace a je asynchronní.

Virtualizované bloky výpočetního výkonu je možno použít ve všech bezpečnostních zónách včetně DMZ.

7.6.4 Unix/Linux server startup rundown

Jednotka zahrnuje služby spojené s instalací nebo s ukončením provozu operačního systému. Provozní doba:11x5

Jednotka přípravy infrastruktury OS zahrnuje zejména následující činnosti:

- Prvotní instalace OS;
- Připojení a konfigurace sítí a diskových prostorů;
- Prvotní konfigurace OS dle požadavků aplikace;
- Instalace bezpečnostních záplat, rozšíření a balíčků;
- Zavedení do konfiguračních databází, provozního a bezpečnostního dohledu, úpravy dokumentace infrastruktury.

Jednotka ukončení infrastruktury OS zahrnuje zejména následující činnosti:

- Zrušení/odinstalace virtuálního serveru;
- Zrušení konfigurace sítí a diskových prostorů;
- Smazání z konfiguračních databází, provozního a bezpečnostního dohledu, úpravy dokumentace infrastruktury;

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

- Předání nebo migrace dat z rušeného serveru.

7.7 Úložný prostor

Úložný prostor je realizován na diskových polích s primárně točivými disky v kombinaci s Flash disky.

Název využívaných jednotek je STOR1 a STOR3.

7.7.1 STOR1

Je služba realizována na diskových polích s primárně točivými disky v kombinaci s Flash disky (cca 10-20 % objemu). Nad oběma druhy datových úložišť pracuje auto-tiering, který se stará o to, aby nejvytěžovanější bloky dat byly umístěny na Flash mediích a byl tak výrazně navýšen reálný výkon úložiště.

7.7.2 STOR3

Je služba realizována točivými disky (600 GB/10k SAS 2,5") organizovanými do RAID-5. STOR3 není vhodný pro více zatížené transakční databáze.

Služby poskytování diskového prostoru zahrnují zejména následující činnosti:

- prvotní zajištění a instalaci HW a firmware diskových polí a SAN;
- konfigurace diskových jednotek a portů, konfigurace a správa RAIDů, tiering, zoningu;
- správu a konfiguraci storage zařízení;
- posouzení vlivu na všechny zákazníky sdílených platforem;
- proaktivní monitoring HW a řešení incidentů;
- preventivní systémovou údržbu;
- aktualizace firmware storage zařízení. (controllery, disky atd) na základě doporučení výrobce a s ohledem na stabilitu provozu;
- konfigurace a správa SAN protokolů a SAN prvků (optika Fibre Channel);
- vytváření a úpravu LUNů a Volumů a jejich mapování pro servery;
- konfigurace a správa virtuálních kontrolerů a virtuálních domén;
- diagnostiku a testování storage zařízení, řešení nestandardních a chybových stavů;
- generování repotů využití kapacit a analýza vytíženosti storage zařízení.

8 SOUČINNOST PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY

- Objednatel stanoví seznam určených osob pro přístup do prostředí nástroje SIEM, tento seznam předá Poskytovateli do 5 pracovních dnů od účinnosti příslušné Objednávky. Objednatel je povinen každou změnu určených osob prokazatelně oznámit Poskytovateli.
- Objednatel stanoví Poskytovateli kontaktní osoby včetně komunikační matice pro případ řešení kybernetických bezpečnostních událostí a incidentů (např. CSIRT tým Objednatele).
- V případě, že Objednatel využívá třetí strany pro správu, servis, podporu, konfiguraci apod. systému/ů monitorovaného/ných v rámci Služby, bude pro zjištění nebo řešení KBU/KBI zajištěna komunikační matice pro přímou komunikaci mezi Poskytovatelem a touto třetí stranou, a to obousměrně. Komunikace bude na straně Poskytovatele zaznamenána a evidována v tiketech v systému Service Desk Poskytovatele. Objednatel bude o této komunikaci dostávat notifikace. Komunikace mezi třetí stranou a Poskytovatelem bude v režimu 24/7. V případě, že třetí strana zjistí KBU/KBI, bude primárně kontaktovat Service Desk Poskytovatele.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

- Objednatel poskytne nezbytnou součinnost Poskytovateli při vytváření výstupů Služby při nominacích kompetentních osob poskytujících součinnost při zpracování výstupů Služby na straně Objednatele a jeho smluvních partnerů. Zejména se jedná o nominace bezpečnostních rolí do realizačních týmů a stanovení jejich potřebných odpovědností a kompetencí s ohledem na poskytovanou Službu;
- Objednatel poskytne nezbytnou součinnost Poskytovateli při zajištění potřebné disponibility nominovaných členů realizačních týmů pro poskytnutí součinnosti s ohledem na odsouhlasené termíny;
- Objednatel poskytne nezbytnou součinnost pro zajištění řádného poskytování služeb Poskytovatelem dle tohoto katalogového listu (e.g. virtualizační prostředky).
- Hlášení poruchy Služby oznamuje Objednatel na Service Desk Poskytovatele.
- Služba Vstupní analýza a Realizace ověření provozu není samostatným Výstupem plnění Služby KL_BM dle kapitoly 3.2. Tyto služby mohou být realizovány na základě samostatných Objednávek, postupem dle Rámcové smlouvy.

9 SMLUVNÍ POKUTY

V případě, že Poskytovatel nesplní některou ze stanovených SLA povinností, tj. stanovené dostupnosti příslušné Služby uvedené v odst. 6 tohoto katalogového listu, je Objednatel oprávněn požadovat smluvní pokutu ve výši 100 % z poměrné části příslušné měsíční Ceny za Službu bez DPH za dobu, kdy příslušná Služba nesplnila stanovené SLA.

V případě prodlení Poskytovatele s odstraněním závady příslušné Služby ve lhůtě stanovené v odst. 6 tohoto katalogového listu, má Objednatel právo uplatnit vůči Poskytovateli smluvní pokutu ve výši 100 % z poměrné části příslušné měsíční Ceny za Službu bez DPH za dobu přesahující hodnotu parametru doby vyřešení kritické závady dané Služby.

V případě prodlení Poskytovatele s dodáním Předmětu plnění specifikovaném v odst. 3.1 a odst. 3.2 tohoto katalogového listu, má Objednatel právo uplatnit vůči Poskytovateli smluvní pokutu, jejíž výše a parametry budou uvedeny v konkrétní Nabídce a následné Objednávce.

10 POUŽITÉ VÝRAZY

Výraz	Popis
SPCSS	Státní pokladna Centrum sdílených služeb, s. p.
SPCSS NDC	Datové centrum SPCSS ve smyslu NDC i DCZ.
OCKB – SPCSS	Odbor Centra Kybernetické Bezpečnosti ve společnosti SPCSS.
Computer Security Incident Response Team (CSIRT–SPCSS)	Bezpečnostní tým ve společnosti SPCSS – zajišťuje spolupráci při řešení bezpečnostních incidentů. Na rozdíl od běžného bezpečnostního týmu je CSIRT zapojen do národní a světové bezpečnostní infrastruktury, která umožňuje sdílení informací a stanovení formálních postupů.
Security Operations Center	Označuje specializované pracoviště v SPCSS, které soustřeďuje složky ochrany informačních dat a systémů. Toto pracoviště využívá k ochraně bezpečnosti celou řadu softwarových a hardwarových systémů, obsahuje celou řadu automatických nástrojů, pro odhalení útoků, které by člověk mohl přehlédnout. Cíl SOC:

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Výraz	Popis
(SOC)	Monitorování a ochrana před pokusy o průnik do systémů. Zajištění souladu činností s právními předpisy, jež se týkají ochrany dat.
Kritická informační infrastruktura (KII)	KII je prvek nebo systém prvků kritické infrastruktury. Narušení jeho funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.
Významný informační systém (VIS)	VIS je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.
ZoKB	Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
VoKB	Vyhláška 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)
Významná sťí	Je síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře.
CSIRT	Computer Security Incident Response Team. Základní povinností každého CSIRT týmu je spolupráce při řešení incidentů („response“).
BH	Bezpečnostní hlášení – jedná se o hlášení zadané do aplikace Service Desk přímo koncovým uživatelem, který má podezření na KBU nebo KBI.
KBU	Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
KBI	Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události. Kategorie III – velmi významný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod, Kategorie II – významný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod, nebo Kategorie I – méně významný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Výraz	Popis
SIEM	Security information and event management se zabývá dlouhodobým ukládáním událostí, jejich analýzou a hlášením problémů.
Offense	Přestupek, porušení pravidel, narušení systému, které detekoval nástroj SIEM.
Intrusion Detection Systems (IDS) Intrusion Prevention Systems (IPS)	Jedná se o systémy, které jsou schopny rozpoznat škodlivé aktivity v síti, zaznamenávat informace spojené s touto aktivitou. K detekci používají sledování anomálií ve využívání síťových protokolů a sledování anomálií provozu jako takového. Hlavní vlastností IPS a IDS je detekce podezřelého chování pomocí signatur. Systém IPS umí vzniklý nebezpečný provoz blokovat, IDS škodlivé chování pouze detekuje.
User behavior analytics (UBA)	Uživatelská behaviorální analýza – využívá zkoumání chování uživatele bez předchozí znalosti osobnosti. Systém vytváří vlastní vzorek každého uživatele a vyhodnocuje změny, které se odklání od obvyklého chování. Např. uživatel provádí aktivitu v takové míře nebo z místa, které neodpovídá předchozímu chování. Naprostá pravidelnost a rychlost, která provází podezřelou činnost, může nasvědčovat, že došlo k odcizení identity a aktivitu provádí škodlivá aplikace, nikoliv člověk.
Forenzní analýza	Prostředek, který pomáhá při řešení bezpečnostních incidentů slouží pro získání důkazů.
NetFlow	Otevřený protokol vyvinutý společností Cisco Systems. Poskytuje informace z třetí a čtvrté vrstvy referenčního modelu ISO/OSI.
NetFlow exportér	Směrovač, přepínač, speciální sonda. Zařízení, které je připojeno k monitorované lince a analyzuje procházející pakety. Na základě zachycených IP toků generuje NetFlow statistiky a ty exportuje na NetFlow kolektor. Využití směrovačů – sledování a zpracování NetFlow informací má vliv na výkon zařízení. Speciální sondy – specializované zařízení neviditelné v síti (instalované do L2), které nezasahuje do provozu. Statistiky jsou obvykle předávány dedikovaným rozhraním.
NetFlow kolektor	NetFlow kolektor je zařízení s velkou úložnou kapacitou, které sbírá statistiky z většího počtu NetFlow exportérů a ukládá je do dlouhodobé databáze.
Informace typu PCI	Payment Card Industry – informace o platebních kartách.
Informace typu PII, SPI	PII – Personally identifying information – osobní informace. SPI – Sensitive personal information – citlivé osobní informace.
Honey pots	Jedná se o „návnadný" systém, který je určen k detekci pokusů neoprávněného použití systémů a detekce podezřelého chování. Systém se tváří jako legitimní systém pro přilákání pozornosti případného útočníka. Všechny aktivity jsou monitorovány.
Podpora L1	První úroveň technické podpory poskytované Poskytovatelem.
Jednotka bezpečnostního monitoringu	Jedná se o hodnotu, která uvádí, kolik událostí dokáže generovat sledovaný systém nebo aplikace během jedné sekundy. Hodnota se může měnit dle zátěže, stavu systému nebo aplikace.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

KATALOGOVÝ LIST – SPRÁVA PRIVILEGOVANÝCH ÚČTŮ

Název služby	**Správa privilegovaných účtů**

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Správa privilegovaných účtů (dále jen **„Služba KL_PU"**) je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL_PU.

Název milníku	**Termín splnění milníku**
Zahájení poskytování Služby KL_PU	Na základě Objednávky
Ukončení poskytování Služby KL_PU	Na základě Objednávky

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba KL_PU bude poskytována v režimu, dle popisu v tabulce:

Režim poskytování Služby KL_PU	**Doba poskytování Služby KL_PU**
Standardní provozní doba – Část 1 a 2	Nepřetržitě (24x7)
Poskytování podpory Služby KL_PU	V pracovní dny (5x8) 8–16 h

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 Vstupy

Vstupy dodané Objednatelem pro Službu KL_PU jsou:

- Relevantní dokumenty Objednatele;
- Vstupní analýza – zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování plnění dle smlouvy uzavřené mezi Poskytovatelem a Objednatelem;

- Realizace ověření provozu – zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování plnění dle smlouvy uzavřené mezi Poskytovatelem a Objednatelem.

3.2 Výstupy

Výstupy Služby KL_PU jsou:

- Poskytování Služby KL_PU;
- měsíční zpráva o stavu služby dle tohoto katalogového listu;
- dokument Nasazení Služby správy privilegovaných účtů v rozsahu Objednávky Objednatele (dokumentace obsahuje také klasifikaci zpracovaných informací, pravidla likvidace dat a exit plán v rozsahu dané Služby).

4 POPIS ROZSAHU SLUŽBY

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, který vychází z doporučené normy ISO/IEC 27001, kde je nutné zavést správu přístupu k privilegovaným účtům a monitoring veškeré aktivity účtů s vazbou na konkrétní osobu, která jím právě disponuje. Využití této Služby KL_PU se doporučuje
i pro ostatní pro Objednatele významné informační systémy. Řešení je poskytováno v režimu vysoké dostupnosti.

Služba Správy privilegovaných účtů obsahuje tyto oblasti:

- **Řízení přístupu privilegovaných účtů** – kontrola přístupu k informačnímu systému pomocí privilegovaných účtů dle požadovaného rozsahu;
- **Session Recording** – zaznamenávání aktivit privilegovaných účtu včetně nahrávek obrazovek a stisků kláves (key-logging);
- **Password Management** – zajišťuje centrální správu privilegovaných účtů se zabezpečeným úložištěm hesel a správou přístupů k těmto účtům;

Část 1 - Standardní součásti Služby KL_PU (nedílné součásti KL_PU, poskytováno vždy)	
☒	Řízení přístupu privilegovaných účtů
☒	Session Recording
Část 2 - Doplňkové služby	
☐	Password Management

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, a to tyto opatření:

- § 19 Správa a ověřování identit;

- § 20 Řízení přístupových oprávnění.

Služba KL_PU nezahrnuje organizační opatření SŘBI Objednatele. Součástí Služby KL_PU dle tohoto katalogového listu není tvorba politik.

5 POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL_PU

5.1 Řízení přístupu

Jedná se o klíčový modul pro řízení životního cyklu privilegovaného uživatele v podniku. Pro minimalizaci úniku citlivých dat jsou v rámci služby využity bezpečnostní principy, auditní nástroje i nástroje reportingu.

Služba poskytuje funkce pro autentizaci privilegovaných uživatelů. Služba zajišťuje přidělování a správu oprávnění uživatelů pro přístup k informačním systémům nejen v rámci podnikové infrastruktury, ale umožňuje napojení cloudových služeb, které Objednatel využívá. Všechna nastavená pravidla jsou kontrolována a analyzována. Služba umožňuje také zjednodušení operativy, která je se správou účtů spojena. Služba nemá pouze funkce, které pomáhají operativě, ale svými funkcemi přináší i uživatelský pracovní komfort.

Služba nabízí nástroje, které umožňují správu identit, změnu rolí, logování aktivit uživatele, implementaci bezpečnostních zásad, to vše lze monitorovat, reportovat i auditovat. Služba zajišťuje efektivní a bezpečné řízení účtů nejen uživatelů, ale i aplikací a skriptů.

Služba obsahuje tyto funkce: Správa privilegovaných účtů a uživatelský provisioning, Federace identit, Přemostění identit, Zajištění soukromí, Single sign-on, Silná autentizace, Paswordless ověření, Správa souhlasu, Řízení přístupu, Analytický modul, Uživatelský portál, API rozhraní, Přihlášení pomocí sociálních sítí, Napojení na Externí identity providery.

Systém je interně spravován pomocí webových služeb SOAP, známých jako admin služby. Systém umožňuje komunikovat pomocí SOAP, ale i REST API, které je primárně doporučováno.

Služba je provozována v režimu vysoké dostupnosti.

Logy získané z Řízení přístupu budou ukládány prostředky Řízení přístupu.

5.2 Session Recording

Tato funkcionalita, zajišťuje spolehlivý záznam všech činností administrátorů, s indexovaným video log záznamy, všech nebo vybraných relací. Session recording lze využít na lokální aktivity správců, aktivity prováděné pomocí vzdálené plochy nebo přes SSH. Záznam se neomezuje jen na záznam obrazovky, ale je k dispozici i audio záznam, který může být využit ke kontrole činnosti dodavatelů. Video log má všechny potřebné informace, aby jej bylo možno využít jako průkazný materiál v případě auditu nebo forensních analýz. Nasazení je realizováno na serveru, přes který jsou všechny administrátorské relace uskutečňovány. Session recording nijak neomezuje práci správců a nevyžaduje žádné změny organizačních procesů.

Monitoring probíhá v reálném čase a podezřelé aktivity ihned notifikuje. Správce, který provádí podezřelou činnost, lze okamžitě zablokovat.

Session recording lze využít pro kontrolu přístupu třetích stran *(partnerů, subdodavatelů, poskytovatelů externích služeb)*.

Session recording, lze využít i k edukaci juniorních správců, kdy si mohou přehrávat záznamy aktivit zkušenějších kolegů.

Logy získané ze Session recordingu budou ukládány prostředky Session recordingu.

6 DOPLŇKOVÉ SLUŽBY

6.1 Password Management

Služba podporuje bezpečné ukládání přihlašovacích údajů. Možnost instalace agentů pro propagaci nové konfigurace skrze celé prostředí. Služba poskytuje možnost sdíleného přístupu k jednotlivým trezorům, umožnění přístupu skupině uživatelů ke sdílenému trezoru pro využití v něm bezpečně uložených hesel. Součástí služby je podrobný auditní log, který je přístupný definované osobě. Služba je provozována v režimu vysoké dostupnosti. Součástí služby je procesní dokumentace pro využívání nástroje Password Management.

Službu Password managementu je možné využít i pro ostatní uživatele, kteří disponují větším počtem přístupových údajů, jenž využívají ke své pracovní činnosti.

6.2 Poskytování podpory pro Službu KL_PU

Jedná se o poskytování podpory související s poskytováním Služby KL_PU. Jedná se zejména o podporu těchto činností:

správa privilegovaných uživatelských účtů (přidání uživatele, odebrání uživatele, změna oprávnění uživatele) na základě požadavku Objednatele.

6.3 Pravidelná zpráva o stavu služby dle tohoto katalogového listu

Zpráva obsahuje tyto informace:

- Období poskytování Služby KL_PU;
- Režim poskytování Služby KL_PU;
- Popis rozsahu Služby KL_PU;
- Provozovaná prostředí;
- Aktivity Služby KL_PU;
- Řízení provozu Služby KL_PU;
- Návrh na nápravná opatření a doporučení.

7 SLA PARAMETRY

Poskytovatel je povinen poskytovat službu KL_PU dle Smlouvy v rozsahu definované objednávkou, a to v níže uvedených parametrech.

Ovlivnění chodu všech částí Služby KL_PU ze strany Objednatele (přerušení komunikace na straně Objednatele, a to úplné nebo částečné a obdobné) a z důvodů mimo působnost Poskytovatele se nezapočítává do nedostupnosti žádné z částí Služby KL_PU.

7.1 Požadovaná měsíční dostupnost Částí Služby – vybraná Část 1 a Část 2

Název Služby:	**Správa privilegovaných účtů**	
SLA parametry		
Část Služby:	**Dostupnost Služby:**	**Servisní okno pro odstávky:**

Název Služby:	**Správa privilegovaných účtů**	
SLA parametry		
Část 1 – Řízení přístupu privilegovaných účtů, Session Recording	99,5 %	každý čtvrtek, vždy 19:00-24:00
Část 2 - Password Management	99,5 %	každý čtvrtek, vždy 19:00-24:00

Tabulka – Řízení přístupu privilegovaných účtů, Session Recording, Password Management

Nedostupnost Služby KL_PU – Část 1 (Řízení přístupu privilegovaných účtů, Session Recording) a Část 2 (Password Management) způsobená hardwarovou nebo jinou technickou závadou se počítá od okamžiku zahájení nedostupnosti Služby KL_PU – Část 1 a Část 2 ve výše definovaném rozsahu do okamžiku obnovení poskytování. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti Služby KL_BM – Část 1 a Část 3 ve výše definovaném rozsahu, počítá se nedostupnost služby od doby jejího nahlášení.

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

7.1.1 Postup výpočtu dostupnosti Služby

Dostupnost služby se vypočítá podle následujícího vzorce:

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

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, mimořádné odstávky a další dle specifické Části Služby KL_PU.

7.1.2 Požadované lhůty pro obnovení Služby KL_PU – Vybraná část Části 1 a Části 2

Název Služby:	**Správa privilegovaných účtů**		
Část Služby:	**Lhůta pro obnovení služby v běžné provozní době v hodinách**		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Část 1 – Řízení přístupu privilegovaných účtů, Session Recording	6	24	168
Část 2 - Password Management	6	24	168

Tabulka – Požadované lhůty pro obnovení Služby KL_PU – vybraná část Části 1 a Část 2

Kategorizace provozních incidentů:	
Incident kategorie A	Služba není dostupná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje její užívání. Tento stav kritickým způsobem omezuje běžný provoz.
Incident kategorie B	Služba, je ve svých funkcích degradována tak, že tento stav zásadně omezuje (Nefunkční dílčí součást v rozsahu vybrané součásti Části 1 a Část 2) její běžný provoz.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

Tabulka – Kategorizace provozních incidentů

7.2 Reakční doby Poskytování podpory Služby KL_PU

Podpora dle Služby KL_PU je určena k zajištění rozvoje a podpory jejího efektivního využívání. Doba reakce na požadovanou podporu Služby KL_PU je počítána od zadání požadavku do aplikace Service Desk Poskytovatele. Za reakci je považována odpověď na požadavek s návrhem dalšího postupu řešení.

Podpora Služby KL_PU je poskytována v režimu 8x5.

Název Služby:	Správa privilegovaných účtů	
SLA parametry		
Podpora Služby KL_PU – Správa privilegovaných účtů (podpora 8x5)	**Maximální doba reakce na požadavek Objednatele**	**Doba vyřešení požadavku**
	Následující pracovní den	Po dohodě obou Smluvních stran

Tabulka č. 2 – Reakční doby a doby podpory Služby KL_PU

7.3 Plánované odstávky

V rámci poskytování Služby KL_PU si Poskytovatel vyhrazuje právo na plánované odstávky celého nebo částí systému z důvodu údržby jak samotného systému, tak infrastruktury a datové konektivity Poskytovatele. Poskytovatel se zavazuje plánované práce s vlivem na dostupnost Služby KL_PU soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL_PU ovlivněna co nejméně.

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

8 SOUČINNOST PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY KL_PU

- Požadavky na podporu v rámci služby Správa privilegovaných účtů jsou Objednatelem zadávány pomocí Service desku SPCSS Oprávněnou osobou nebo určenou osobou.
- Objednatel stanoví Poskytovateli kontaktní osoby včetně komunikační matice pro případ řešení bezpečnostních událostí a incidentů;
- Objednatel poskytne nezbytnou součinnost Poskytovateli při vytváření výstupů Služby při nominacích kompetentních osob poskytujících součinnost při zpracování výstupů Služby na straně Objednatele a jeho smluvních partnerů;
- Objednatel poskytne nezbytnou součinnost Poskytovateli při zajištění potřebné disponibility nominovaných členů realizačních týmů pro poskytnutí součinnosti s ohledem na odsouhlasené termíny;
- Objednatel poskytne nezbytnou součinnost pro zajištění řádného poskytování služeb Poskytovatelem dle tohoto katalogového listu.
- Služba Vstupní analýza a Realizace ověření provozu není samostatným Výstupem plnění Služby KL_PU dle kapitoly 3.2. Tyto služby mohou být realizovány na základě samostatných Objednávek, postupem dle Rámcové smlouvy.

9 SMLUVNÍ POKUTY

V případě, že Poskytovatel nesplní některou ze stanovených SLA povinností, tj. stanovené dostupnosti příslušné Služby uvedené v odst. 7 tohoto katalogového listu, je Objednatel oprávněn požadovat smluvní pokutu ve výši 100 % z poměrné části příslušné měsíční Ceny za Službu bez DPH za dobu, kdy příslušná Služba nesplnila stanovené SLA.

V případě prodlení Poskytovatele s odstraněním závady příslušné Služby ve lhůtě stanovené v odst. 7 tohoto katalogového listu, má Objednatel právo uplatnit vůči Poskytovateli smluvní pokutu ve výši 100 % z poměrné části příslušné měsíční Ceny za Službu bez DPH za dobu přesahující hodnotu parametru doby vyřešení kritické závady dané Služby.

10 POUŽITÉ VÝRAZY

Výraz	Popis
SPCSS	Státní pokladna Centrum sdílených služeb, s. p.
OCKB – SPCSS	Odbor Centra Kybernetické Bezpečnosti v SPCSS.
Zákon č. 181/2014 Sb.	ZoKB – Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
Vyhláška č. 82/2018 Sb.	VoKB – Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (Vyhláška o kybernetické bezpečnosti).
Kritická informační infrastruktura (KII)	KII je prvek nebo systém prvků kritické infrastruktury. Narušení jeho funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.
Významný informační systém (VIS)	VIS je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.
NDC SPCSS	Národní datové centrum, Státní pokladna Centrum sdílených služeb, s.p.

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

KATALOGOVÝ LIST – VULNERABILITY MANAGEMENT

Název služby	**Vulnerability management**

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Vulnerability management (dále jen **„Služba KL_VM"**) je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL_VM.

Název milníku	**Termín splnění milníku**
Zahájení poskytování Služby KL_VM	Na základě Objednávky
Ukončení poskytování Služby KL_VM	Na základě Objednávky

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba KL_VM bude poskytována v režimu, dle popisu v tabulce:

Režim poskytování Služby KL_VM	**Doba poskytování Služby KL_VM**
Standardní provozní doba služby (periodický sken)	1x měsíčně
Standardní provozní doba služby (Ad-hoc sken)	V pracovní dny (5x8) 8–16 h

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 Vstupy

Vstupy dodané Objednatelem pro Službu KL_VM jsou:

- Relevantní dokumenty Objednatele;
- Vstupní analýza – zpracovaná Dodavatelem a předaná Objednateli v rámci poskytování odpovídajícího plnění;
- Realizace ověření provozu – zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování plnění.

3.2 Výstupy

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Výstupy Služby KL_VM jsou:

- Poskytování Služby KL_VM;
- měsíční zpráva o stavu služby dle tohoto katalogového listu;
- dokumentace Nasazení Služby Vulnerability managementu v rozsahu Objednávky Objednatele.

4 POPIS ROZSAHU SLUŽBY

Služba KL_VM je podpůrné řešení v minimalizaci výskytu zranitelností v celé ICT infrastruktuře a slouží jako nástroj i pro naplnění legislativních požadavků podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále také „VoKB").

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

Služba KL_VM 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 KL_VM. 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 KL_VM probíhá dle metodiky NIST.

Služba KL_VM snižuje nároky na zdroje Objednatele pro včasnou kontrolu a ověřování zranitelností. Prostřednictvím této služby je dosahována vysoká kvalita Vulnerability managementu pro aktiva Objednatele. Součástí služby je poskytování přehledného reportingu.

Službu KL_VM lze provozovat v perimetru Objednatele, i z prostředí SPCSS, viz. Doplňkové služby. Při nasazení služby v perimetru Objednatele je nezbytné zajistit odpovídající součinnost.

Vysoká dynamika výskytu bezpečnostních zranitelností a jejich možné zneužití vyžaduje komplexní službu Vulnerability managementu pro minimalizaci rizik při řešení ochrany infrastruktury Objednatele.

Služba KL_VM je rozdělena do dvou částí:

Část 1 a **Část 2** jsou určeny k zajištění povinností stanovených příslušnou legislativou, blíže popsáno v kapitole 4.1. Tyto části jsou poskytovány vždy.

Část 3 obsahuje Doplňkové služby, které jsou nezbytné k řádnému poskytování služby, a to dle požadované architektury, která je určena na základě Vstupní analýzy dle kapitoly 3.1.

Část 1 - Součásti služby Vulnerability management povinné k naplnění vybraných opatření (nedílné součásti KL_VM, poskytováno vždy)	
☒	Příprava a průběžná úprava skenovacích scénářů
☒	Počáteční inicializační sken
☒	Periodický sken
☒	Ad-hoc sken
☒	Zpracování zprávy o stavu Služby KL_VM dle tohoto katalogového listu určené Objednateli (předávána v měsíčním intervalu)

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Část 2 – Ostatní součásti služby Vulnerability management povinné k naplnění vybraných opatření (nedílné součásti KL_VM, poskytováno vždy)	
☒	Vulnerability management – Konzole
☒	Vulnerability management – Engine
Část 3 - Doplňkové služby – Vulnerability management	
☐	Virtualizační prostředí pro provozování Služby KL_VM v prostředí SPCSS

4.1 Plnění legislativních povinností Objednatele

Služba KL_VM je podpůrným prostředkem pro naplnění povinností definovaných zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, v platném znění, resp. vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti. KL_VM obsahuje obecný výčet požadavků VoKB, pro jejichž naplnění Objednateli služba KL_VM poskytuje informace. Specifika dle klasifikace informací a povahy spravovaného systému (jako KII, VIS) jsou ze strany Objednatele určeny Objednávkou, specifikovány Vstupy dle kapitoly 3.1 a budou zaznamenány v dokumentu „Nasazení Služby Vulnerability management v rozsahu Objednávky Objednatele" dle kapitoly 3.2.

Jedná se o tyto paragrafy VoKB:

§ 5 Řízení rizik

Služba KL_VM pomáhá při identifikaci relevantních hrozeb a zranitelností u jednotlivých aktiv. Výsledky skenování zranitelností pomáhají při zohlednění relevantních hrozeb při dopadu na aktiva.

§ 10 Řízení provozu a komunikací

Výstupy služby KL_VM pomáhají při stanovení provozních pravidel a postupů určených pro zajišťování bezpečného provozu informačního a komunikačního systému.

§ 11 Řízení změn

V případě významných změn informačního systému, je prováděna analýza rizik (není součástí Služby KL_VM), kdy na základě výsledku Povinná osoba (Objednatel) rozhoduje o provedení testu zranitelností a reaguje na zjištěné nedostatky.

§ 14 Zvládání kybernetických bezpečnostních událostí a incidentů

V rámci zvládání kybernetických bezpečnostních událostí a incidentů, zajistí Povinná osoba (Objednatel) aby uživatelé, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti.

§ 28 Průmyslové, řídicí a obdobné specifické systémy

Zajištění kybernetické bezpečnosti pomocí nástrojů a opatření pro ochranu jednotlivých technických aktiv těchto systémů před využitím známých zranitelností.

Služba KL_VM nezahrnuje organizační a technická opatření SŘBI Objednatele. Součástí Služby KL_VM není tvorba politik, vyjma dokumentace dle kapitoly 3 tohoto katalogového listu. Služba KL_VM nepokrývá výše zmíněné ustanovení VoKB v plném rozsahu, ale výstupy Služby KL_VM jsou využívány při realizaci jednotlivých organizačních a technických opatření v rámci SŘBI Objednatele.

5 POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL_VM

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Předmětem Služby KL_VM je skenování zranitelností probíhající jedenkrát měsíčně nebo manuálním Ad-hoc skenem. Služba KL_VM se skládá z:

- Komponenty služby KL_VM
- Fáze služby KL_VM

5.1 Komponenty Služby KL_VM

Jednotlivé komponenty Služby KL_VM:

- Vulnerability management – Konzole

  Jedná se o část systému, která slouží ke správě systému a poskytuje funkce pro vyhodnocování nálezů, správu skenovacích scénářů a evidenci zranitelností.

- Vulnerability management – Engine

  Je část systému instalovaná ve vybrané části perimetru Objednatele, tak aby umožnila získání relevantních informací o skenovaných systémech. Tato část může být současně instalována na několika místech v perimetru Objednatele. Umístění a počty této komponenty bude stanoveno na základě analýzy dle kapitoly 3.1.

- Vulnerability management je prováděn expertním týmem SOC SPCSS.

5.2 Realizace Služby KL_VM

Jednotlivé kroky poskytování Služby KL_VM:

- 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 katalogového listu.

5.2.1 Příprava a průběžná úprava skenovacích scénářů

Klíčovou činností pro správnou funkcionalitu služby je příprava skenovacích scénářů. Tato příprava skenovacích scénářů probíhá v součinnosti se zástupci Objednatele (obvykle se jedná o správce informačních systémů, manažery kybernetické bezpečnosti). Objednatel definuje typ, rozsah i skupiny aktiv, ale i čas kdy bude daný sken probíhat. Návrhy jsou následně konzultovány s pracovníky Dodavatele. Součástí přípravy je i identifikace aktiv, která mohou být ze skenování vyňata. Definice skenovacích scénářů je součástí dokumentace „Nasazení Služby Vulnerability managementu v rozsahu Objednávky Objednatele".

5.2.2 Počáteční Inicializační sken

Počáteční inicializační sken je specifický četností identifikovaných nálezů. Jeho provedení je časově náročnější při přípravě a zpracování výstupů, které jsou dále předávány Objednateli.

- Sken, který je spuštěn při nasazení služby nebo v případě rozšíření skupiny skenovaných aktiv. Sken slouží k prvotnímu nálezu zranitelností ICT infrastruktury.
- Z důvodu možného vysokého počtu nálezů je zpracování výsledků časově náročnější.
- Může se vyskytovat zvýšená interakce mezi Dodavatelem a Objednatelem.

5.2.3 Periodický sken

Periodicky se opakující skeny jsou prováděny automaticky v předem stanovených dnech a časech.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

- Periodicky se opakující sken by měl generovat menší počet nálezů zranitelností, oproti inicializačnímu skenování v případě, že nálezy z inicializačního skenování jsou vypořádány.
- Pravidelné skenování množiny prvků ICT infrastruktury v předem definovaných termínech.

5.2.4 Ad-hoc sken prováděný na vyžádání

Tyto skeny jsou prováděny manuálně a jsou vyvolané jako reakce na vnější podněty, jako:

- Ověření nasazených bezpečnostních opatření, které byly aplikovány na nalezené zranitelnosti.
- Významná změna informačního systému.
- Zveřejnění informace o kritické zranitelnosti, která se týká sledovaných informačních systémů.

Tento typ skenování je realizován jednorázově na základě požadavku Objednatele a dle vzájemně dohodnutého Ad-hoc scénáře.

5.3 Pravidelná zpráva o stavu služby dle tohoto katalogového listu

Zpráva obsahuje tyto informace:

- Období poskytování Služby KL_VM;
- Režim poskytování Služby KL_VM;
- Popis rozsahu Služby KL_VM;
- Seznam aktiv skenovaných službou KL_VM včetně jejich detailního popisu;
- Přehled výskytu zranitelností zjištěných službou KL_VM;
- Přehled závažných zranitelností podle operačních systémů zjištěných službou KL_VM;
- Výpis závažných zranitelností (úroveň zranitelnosti 8-10) zjištěných službou KL_VM;
- Výpis zranitelností nižší úrovně zjištěných službou KL_VM;
- Přehled Ad-hoc skenů provedených v rámci služby KL_VM;
- Doporučení, jak zjištěné zranitelnosti řešit.

5.4 Cílová prostředí

Službu KL_VM 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.

Definice cílového prostředí pro poskytování Služby KL_VM bude stanovena na základě analýzy dle kapitoly 3.1.

6 SLA PARAMETRY

Poskytovatel je povinen poskytovat Službu KL_VM dle Smlouvy v rozsahu definovaném objednávkou, a to v níže uvedených parametrech.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Ovlivnění chodu všech částí Služby KL_VM ze strany Objednatele (přerušení komunikace na straně Objednatele, a to úplné nebo částečné, nedostatečné zajištění součinnosti a obdobné) a z důvodů mimo působnost Poskytovatele se nezapočítává do nedostupnosti žádné z částí Služby KL_VM.

6.1 Požadovaná měsíční dostupnost částí služby – Vybraná Část 1

Název Služby:	**Vulnerability management**	
SLA parametry		
Část Služby:	**Dostupnost Služby:**	**Servisní okno pro odstávky:**
Část 1 – Periodický sken	1x měsíčně	každý čtvrtek vždy 19:00-24:00
Část 1 – Ad-hoc sken	až 10x měsíčně	každý čtvrtek vždy 19:00-24:00

Tabulka – Požadovaná měsíční dostupnost částí služby – Část 1

Nedostupnost součástí Služby KL_VM – Příprava a průběžná úprava skenovacích scénářů, Počáteční inicializační sken, Kontrolní sken, Zpracování zprávy o stavu Služby KL_VM dle tohoto katalogového listu určené Objednateli (předávána v měsíčním intervalu) - neovlivňuje dostupnost a kvalitu poskytované Služby KL_VM ve výše definovaném rozsahu a nemá tak vliv na plnění příslušného SLA.

Část 1 - Ad-hoc sken je realizován vždy jednorázově na základě požadavku Objednatele a dle vzájemně dohodnutého Ad-hoc scénáře. Objednatel má v rámci daného období (1 měsíc) nárok na realizaci až 10x Ad-hoc sken. Nevyčerpané Ad-hoc skeny se nepřevádí do dalšího období (následující měsíc).

6.2 Požadovaná měsíční dostupnost částí služby – Vybraná Část 2

Název Služby:	**Vulnerability management**	
SLA parametry		
Část Služby:	**Dostupnost Služby:**	**Servisní okno pro odstávky:**
Část 2 – Vulnerability management – Konzole	až 11x měsíčně	každý čtvrtek vždy 19:00-24:00
Část 2 – Vulnerability management – Engine	až 11x měsíčně	každý čtvrtek vždy 19:00-24:00

Tabulka – Požadovaná měsíční dostupnost částí služby – Část 2

6.3 Reakční doby a doby Služby KL_VM

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Doba reakce je počítána od zaevidování požadavku na provedení Ad-hoc skenování do aplikace Service Desk SPCSS (servicedesk.spcss.cz). Dodavatel musí do doby uvedené v tabulce níže přijmout k řešení požadavek na Ad-hoc skenování v aplikaci Service Desk. Reakční doba není stanovena pro provedení Část 1 - Periodický sken.

Název Služby:	**Vulnerability management**	
SLA parametry		
Část Služby:	**Maximální doba reakce na požadavek Objednatele**	**Doba vyřešení požadavku**
Část 1 – Ad-hoc sken	Do 24 hodin od doby přijetí požadavku	Do 24 hodin od doby reakce na požadavek

Tabulka – Reakční doby a doby vyřešení požadavku

Doba reakce na požadavek Objednatele je počítána v režimu 5x8, dle kapitoly 2 – Režim poskytování služby. V případě obdržení požadavku v pracovní den, který předchází dni pracovního klidu, je reakce na požadavek odeslána následující pracovní den.

Maximální doba pro vyřešení požadavku v oblasti Část 1 – Ad-hoc sken platí v případě, že je z požadavku zřejmé, co Objednatel požaduje a že dodal úplné podklady pro vyřešení požadavku. V opačném případě se doba vyřešení požadavku prodlužuje o dobu potřebnou k vyjasnění požadavku nebo doplnění podkladů Objednatelem.

6.4 Plánované odstávky

V rámci poskytování Služby KL_VM 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 Služby KL_VM soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL_VM ovlivněna co nejméně.

Plánované odstávky jsou, pokud možno, soustředěny do servisních oken, která jsou každý čtvrtek v čase 19:00 až 24:00. Ve výjimečných případech jsou odstávky Služby KL_VM realizovány i mimo tato servisní okna. Za ohlášení se považuje informování určených osob Objednatele e-mailem, a to minimálně 24h před zahájením mimořádné odstávky. Doba odstávky, která byla předem řádně ohlášena, se nezapočítává do nedostupnosti Služby KL_VM. Ovlivnění chodu Služby KL_VM ze strany Objednatele se nezapočítává do nedostupnosti Služby KL_VM.

7 DOPLŇKOVÉ SLUŽBY

7.1 Virtualizační prostředí pro provozování služby v prostředí SPCSS

Doplňková služba slouží k zajištění a provozování virtualizovaného prostředí Služby KL_VM v případě realizace v prostředí SPCSS NDC.

Požadovaný rozsah zdrojů virtualizace je specifikován na základě Vstupní analýzy dle kapitoly 3.1.

Standardem je platforma x86, 64bit. Virtualizační platforma je provozována na technologii VMware v minimální verzi VMware vSphere 6.7. Součástí služby jsou SW licence virtualizační platformy a aktualizace verzí virtualizačního SW. Na úrovni virtualizace jsou fyzické core mapovány na virtuální CPU (vCPU). Poměr agregace vCPU 10:1 core a zajištění alokace výkonu 1 vCPU odpovídajícího výkonu 1

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

fyzického core je realizováno prostředky VMware a je v odpovědnosti Dodavatele. Mapování RAM: vRAM je 1:1.

Prostředí se skládá z těchto jednotek:

7.1.1 Building block

Základní stavební jednotkou je Building block (dále také „BB“). Pro provoz virtuálních systémů UNIX/Linux je stanoven BB s poměrem 1:2 (1 vCPU + 2 GB vRAM).

7.1.2 BB – Replikované jednotky

Replikované varianty jednotek zajišťují vysokou dostupnost prostředky virtualizační platformy. Ke každému BB je alokován záložní BB ve druhém DC. V případě výpadku zdrojů v jednom DC dojde k obnovení provozu v druhém DC. Replikace se provádí na úrovni virtuálních serverů (tj. všechny BB jednoho virtuálního serveru musí být replikované) a předpokladem je rovněž zdvojená konfigurace všech diskových prostorů STOR1 nebo STOR3 daného virtuálního serveru. Replikace diskových prostorů do druhého DC se provádí prostředky virtualizace a je asynchronní.

Virtualizované bloky výpočetního výkonu je možno použít ve všech bezpečnostních zónách včetně DMZ.

7.1.3 Unix-Linux High

Správa operačních systémů různých typů (Unix, Linux) včetně využití externí L3 podpory operačních systémů.

Jednotka obsahuje správu operačních systémů na úrovni fyzických i virtuálních serverů. Administrátorské účty OS jsou v rukou Dodavatele. Objednatel používá pro implementaci a podporu provozu aplikací uživatelské účty, využití administrátorských účtů je možné pouze se součinností Dodavatele nebo bezpečným mechanismem schváleným Dodavatelem.

Služba zahrnuje následující činnosti:

- 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;
- 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 naplněnost);
- Komunikace a řešení problémů s externí L3 podporou.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

7.1.4 Unix/Linux server Startup/Rundown

Jednotka zahrnuje služby spojené s instalací nebo s ukončením provozu operačního systému.

Jednotka přípravy infrastruktury OS zahrnuje zejména následující činnosti:

- Prvotní instalace OS;
- Připojení a konfigurace sítí a diskových prostorů;
- Prvotní konfigurace OS dle požadavků aplikace;
- Instalace bezpečnostních záplat, rozšíření a balíčků;
- Zavedení do konfiguračních databází, provozního a bezpečnostního dohledu, úpravy dokumentace infrastruktury.

Jednotka ukončení infrastruktury OS zahrnuje zejména následující činnosti:

- Zrušení/odinstalace virtuálního serveru;
- Zrušení konfigurace sítí a diskových prostorů;
- Smazání z konfiguračních databází, provozního a bezpečnostního dohledu, úpravy dokumentace infrastruktury;
- Předání nebo migrace dat z rušeného serveru.

7.2 Úložný prostor

Úložný prostor je realizován na diskových polích s primárně točivými disky v kombinaci s Flash disky. Název využívaných jednotek je STOR1 – Virtualizovaný a STOR3.

7.2.1 STOR1 – Virtualizovaný

Je služba realizována na diskových polích s primárně točivými disky v kombinaci s Flash disky (cca 10-20 % objemu). Nad oběma druhy datových úložišť pracuje auto-tiering, který se stará o to, aby nejvytěžovanější bloky dat byly umístěny na Flash mediích a byl tak výrazně navýšen reálný výkon úložiště.

7.2.2 STOR3

Je služba realizována točivými disky (600 GB/10k SAS 2,5") organizovanými do RAID-5. STOR3 není vhodný pro více zatížené transakční databáze.

Služby poskytování diskového prostoru zahrnují zejména následující činnosti:

- prvotní zajištění a instalaci HW a firmware diskových polí a SAN;
- konfigurace diskových jednotek a portů, konfigurace a správa RAIDů, tiering, zoningu;
- správu a konfiguraci storage zařízení;
- posouzení vlivu na všechny Objednately sdílených platforem;
- proaktivní monitoring HW a řešení incidentů;
- preventivní systémovou údržbu;
- aktualizace firmware storage zařízení. (controllery, disky atd) na základě doporučení výrobce a s ohledem na stabilitu provozu;
- konfigurace a správa SAN protokolů a SAN prvků (optika Fibre Channel);
- vytváření a úpravu LUNů a Volumů a jejich mapování pro servery;
- konfigurace a správa virtuálních kontrolerů a virtuálních domén;

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

- diagnostiku a testování storage zařízení, řešení nestandardních a chybových stavů;
- generování repotů využití kapacit a analýza vytíženosti storage zařízení.

8 SOUČINNOST PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY

Tato část specifikuje nezbytnou součinnost ze strany Objednatele:

- Objednatel stanoví Poskytovateli kontaktní osoby včetně komunikační matice pro řádné poskytování Služby KL_VM.
- V případě, že Objednatel využívá třetí strany pro správu, servis, podporu, konfiguraci apod. systému/ů skenovaného/ných v rámci Služby KL_VM, bude pro řádné poskytování Služby KL_VM zajištěna ze strany Objednatele komunikace s třetí stranou pro řádné poskytování služby.
- Objednatel poskytne nezbytnou součinnost Poskytovateli při vytváření výstupů Služby při nominacích kompetentních osob poskytujících součinnost při zpracování výstupů Služby na straně Objednatele a jeho smluvních partnerů. Zejména se jedná o nominace bezpečnostních rolí do realizačních týmů a stanovení jejich potřebných odpovědností a kompetencí s ohledem na poskytovanou Službu.
- Objednatel poskytne nezbytnou součinnost Poskytovateli při zajištění potřebné disponibility nominovaných členů realizačních týmů pro poskytnutí součinnosti s ohledem na odsouhlasené termíny.
- Objednatel poskytne nezbytnou součinnost pro zajištění řádného poskytování služeb Poskytovatelem dle tohoto katalogového listu (e.g. virtualizační prostředky).
- Hlášení poruchy Služby oznamuje Objednatel na Service Desk Poskytovatele.
- Objednatel předá informace o skenovaných aktivech a zajistí přístupové údaje pro skenování s přihlášením (pokud je požadováno).
- Objednatel označí aktiva, která jsou vyjmuta ze skenování.
- Služba Vstupní analýza a Realizace ověření provozu není samostatným Výstupem plnění Služby KL_VM dle kapitoly 3.2. Tyto služby mohou být realizovány na základě samostatných Objednávek, postupem dle Rámcové smlouvy.

9 SMLUVNÍ POKUTY

V případě, že Poskytovatel nesplní některou ze stanovených SLA povinností, tj. stanovené dostupnosti příslušné Služby uvedené v odst. 6 tohoto katalogového listu, je Objednatel oprávněn požadovat smluvní pokutu ve výši 100 % z poměrné části příslušné měsíční Ceny za Službu bez DPH za dobu, kdy příslušná Služba nesplnila stanovené SLA.

V případě prodlení Poskytovatele s odstraněním závady příslušné Služby ve lhůtě stanovené v odst. 6 tohoto katalogového listu, má Objednatel právo uplatnit vůči Poskytovateli smluvní pokutu ve výši 100 % z poměrné části příslušné měsíční Ceny za Službu bez DPH za dobu přesahující hodnotu parametru doby vyřešení kritické závady dané Služby.

10 POUŽITÉ VÝRAZY

Výraz	Popis
SPCSS	Státní pokladna Centrum sdílených služeb, s. p.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Výraz	Popis
Kritická informační infrastruktura (KII)	KII je prvek nebo systém prvků kritické infrastruktury. Narušení jeho funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.
Významný informační systém (VIS)	VIS je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.
ZoKB	Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
VoKB	Vyhláška 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)
BH	Bezpečnostní hlášení – jedná se o hlášení zadané do aplikace Service Desk přímo koncovým uživatelem, který má podezření na KBU nebo KBI.
KBU	Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
NIST	The National Institute of Standards and Technology

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

KATALOGOVÝ LIST – KOMPETENČNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI

Název služby	**Kompetenční centrum kybernetické bezpečnosti**

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Kompetenční centrum kybernetické bezpečnosti (dále také **„Služba KL_KC"**) je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL_KC.

Název milníku	**Termín splnění milníku**
Zahájení poskytování Služby KL_KC	Na základě Objednávky
Ukončení poskytování Služby KL_KC	Na základě Objednávky

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba KL_KC bude poskytována v režimu dle popisu v tabulce:

Režim poskytování Služby KL_KC	**Doba poskytování Služby KL_KC**
Standardní provozní doba	V pracovní dny (5x8) 8–16 h

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 Vstupy

Vstupy dodané Objednatelem pro Službu KL_KC jsou:

- Relevantní dokumenty Objednatele včetně požadavků dle kap. 5;
- Vstupní analýza – zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování plnění dle smlouvy uzavřené mezi Poskytovatelem a Objednatelem;
- Realizace ověření provozu – zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování plnění dle smlouvy uzavřené mezi Poskytovatelem a Objednatelem.

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

3.2 Výstupy

Výstupy Služby KL_KC jsou:

- Poskytování Služby KL_KC;
- měsíční zpráva o stavu služby v souladu s kapitolou 5.3 tohoto katalogového listu;
- výstupy na základě požadavku dle kapitoly 5 tohoto katalogového listu;
- dokumentace Nasazení Služby Kompetenčního centra kybernetické bezpečnosti v rozsahu Objednávky Objednatele (dokumentace obsahuje také klasifikaci zpracovaných informací, pravidla likvidace dat a exit plán v rozsahu dané Služby, stanovený roční plán činností pro zpracování v rámci Služby KL_KC definovaný Objednatelem).

Na základě požadavku Objednatele jsou poskytovány informace v souladu s kapitolou 6 tohoto katalogového listu, které musí být vypořádány bez zbytečného odkladu.

4 POPIS ROZSAHU 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).

Část 1 - Součásti služby Kompetenční centrum kybernetické bezpečnosti (nedílné součásti KL_KC, poskytováno vždy)	
☒	Administrace v Nástroji pro podporu řízení SŘBI
☒	Metodická podpora Objednatele
Část 2 - Doplňkové služby	
☐	Administrativní podpora v oblasti Ochrany osobních údajů dle ZoKB
☐	Zvyšování bezpečnostního povědomí

Tabulka – Části služby KL_KC – Část 1 a Část 2

Služba KL_KC je služba postavená na týmu odborníků pokrývajícím všechny potřebné kompetence a znalosti se zajištěnou zastupitelností.

Služba KL_KC je určena jako odborná administrativní podpora v oblasti informační a kybernetické bezpečnosti pro Objednatele. Služba KL_KC zajišťuje podporu vedení a správy systému řízení bezpečnosti informací (dále také „**SŘBI**"). Služba KL_KC Objednateli zajišťuje podporu pro realizaci potřebné agendy v požadovaném čase.

Služba využívá sofistikovaný nástroj 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.

5 POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL_KC

Služba KL_KC zahrnuje:

- administraci dokumentace Objednatele v Nástroji pro podporu řízení SŘBI;
- metodickou podporu Objednatele;

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

- doplňkové služby.

5.1 Administrace v Nástroji pro podporu řízení SŘBI

Na základě konkrétních dodaných podkladů od Objednatele je udržována aktuální evidence klíčové agendy kybernetické bezpečnosti v Nástroji, čímž je zajištěn přehled Objednatele o povinných činnostech v rámci dotčené oblasti SŘBI. Oblastí SŘBI Objednatele je myšlena ta část agendy / informačního systému, která podléhá stejným pravidlům/politikám. Objednatel je pak dle nastavených pravidel v Nástroji automatizovaně notifikován při přednastavené změně stavu. Příkladem může být upozornění Objednatele na nutnost provádět různé aktivity v požadovaném čase, případně je mu poskytnuta informace o jejich nesplnění apod.

Služba KL_KC zahrnuje:

správu evidence bezpečnostních událostí / incidentů a správu plánu zvládání incidentu / události na základě podkladů Objednatele, včetně zajištění evidence souvisejících informací a vyhodnocení;

správu vztahů a vazeb v Nástroji mezi atributy z oblasti informační a kybernetické bezpečnosti dodanými ze strany Objednatele (aktiva, hrozby, zranitelnosti, četnost bezpečnostních událostí / incidentů a zavedená opatření s jejich propadem až do analýzy rizik) i pro účely vizualizace;

správa cílů v Nástroji na základě podkladů dodaných Objednatelem;

správa katalogu bezpečnostních opatření dodaných Objednatelem v Nástroji;

evidenci interních / externích auditů, auditních plánů, auditních zjištění, zvládání auditních zjištění dodaných Objednatelem včetně notifikací osob, které mají získat informace o auditu dle požadavků Objednatele;

zajištění evidence kontrol, kontrolních zjištění a jejich zvládání dodaných Objednatelem včetně notifikací osob, které mají získat informace o kontrole dle požadavků Objednatele;

správa dokumentace SŘBI v Nástroji v podporovaném formátu dokumentu;

nastavení struktury a složek úložiště dokumentace SŘBI a parametrů spravovaných dokumentů (data platnosti, klasifikační stupně, oprávnění k přístupu, notifikace uživatelů, workflow pro připomínkování a schvalování dokumentů apod.) v Nástroji;

nastavení oprávnění, správu rolí až pro 200 uživatelů a nastavení Nástroje dle prostředí Objednatele.

Dokumentem, pro potřeby Služby KL_KC, 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, která není ukládaná v jiném modulu (jako např. Zprávy z jednání VŘKB).

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.

Dokumenty, které se přikládají jako příloha záznamu do jiného modulu (např. Zprávy z auditu v modulu Audit), se do tohoto počtu nezahrnují; nakládání s nimi je součástí úkonů typických pro daný Modul.

Dokumenty v Nástroji vznikají:

1) vložením souboru dokumentu v digitální formě do modulu,
2) vytvořením dokumentu dle předem definované šablony přímo v integrovaném editoru Nástroje v modulu Dokumentace.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Množství spravovaných dokumentů bude stanoveno na základě výstupu ze Vstupní analýzy dle kapitoly 3.1 s předpokladem, že bude 1x ročně provedena revize a aktualizace každého z vložených dokumentů (tedy úprava již vloženého dokumentu nebo jeho nahrazení nově vzniklým dokumentem a následným připomínkováním dokumentu).

Každá samostatná část dokumentace SŘBI Objednatele pro určené VIS/KII nebo ostatní IS Objednatele bude spravována odděleně s tím, že množství vložených dokumentů bude určeno na základě Vstupní analýzy dle kapitoly 3.1. a pro účely stanovení ceny bude Dokumentace SŘBI Objednatele v každé takové části zahrnovat vždy nejméně 34 dokumentů (viz výše). Dokumenty evidované v souhrnné oblasti jako kumulované za jednotlivá SŘBI Objednatele nejsou považovány za nové dokumenty a nebudou tedy počítány do limitu souhrnného SŘBI Objednatele.

Nástroj pro podporu řízení SŘBI

Služba KL_KC využívá Nástroj pro podporu řízení SŘBI. Potřebné informace SŘBI včetně dokumentace jsou administrovány s podporou Nástroje, který vyhovuje potřebám organizací, kde je povinná evidence tak rozsáhlá, že je neefektivní je spravovat pomocí kancelářských aplikací (MS Word, MS Excel atd.). Služba KL_KC umožňuje spravovat a evidovat rozsáhlé oblasti norem a zákonů na jednom místě a poskytovat rozličné přehledy a výstupy s viditelnými vazbami jednotlivých oblastí SŘBI.

Nástroj slouží manažerům pro získání přehledu o všech povinných činnostech. Přístup do Nástroje je určen zejména pro bezpečnostní role dle ZoKB a další odpovědné osoby dle požadavku Objednatele v počtu do 200 uživatelů, volitelně je možné navýšit počet až na 500 uživatelů. Navýšení je možné pouze v případě synchronizace uživatelů napojením na systém pro autentizaci uživatelů Objednatele (např. Active Directory). Nástroj formou notifikací upozorňuje na termíny plnění a průběžný stav jednotlivých aktivit.

Nástroj vznikl, a je i nadále rozvíjen, na základě praxe certifikačních auditorů, čímž se vytvořila struktura, kterou auditor při auditu požaduje a není třeba připravovat další dokumentaci na audit.

Nástroj je modulární a je možné jej v rámci implementace přizpůsobit standardům a procesům Objednatele.

SPCSS využívá Nástroj jako nedílnou součást Služby KL_KC. 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 KL_KC.

Nástroj je umístěn v prostředí SPCSS, které poskytuje vysokou kvalitu služeb a vysokou úroveň zabezpečení (Bezpečné datové centrum).

Nedostupnost Nástroje není překážkou pro poskytování Služby KL_KC. Objednatel zadává požadavky do aplikace Service Desk SPCSS (Poskytovatele) a požadavek bude vyřešen Poskytovatelem.

Moduly Nástroje:

- Aktiva/hrozby/opatření;
- Cíle;
- Audity a kontroly;
- Bezpečnostní incidenty a události;
- Rizikové scénáře;
- Analýzy rizik;
- Třetí strany – Evidence dodavatelů i odběratelů;
- Řízení dokumentace.

5.2 Metodická podpora Objednatele

Součástí Služby KL_KC je metodická podpora Objednatele v oblasti informační a kybernetické bezpečnosti. Podporu poskytují odborníci SPCSS.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Metodická podpora se soustřeďuje zejména na povinnosti vyplývající z oblasti SŘBI a informační a kybernetické bezpečnosti Objednatele. Jedná se zejména o podporu těchto činností:

- metodická, procesní a dokumentační podpora v oblasti, včetně tvorby související dokumentace; vypracování analýz pro podporu rozhodování Objednatele nebo zpracování návrhů řešení;
- podpora zvládání KBU / KBI (při detekci, vyhodnocení, procesu řízení a evidenci);
- návrh koncepčního rozvoje a návrh architektury komunikačních a informačních systémů;
- návrhy, vhodnost použití bezpečnostních opatření a možnosti jejich nasazení;
- definice cílů řízení bezpečnosti informací a jejich prioritizace;
- pomoc při vypořádání nálezů a nastavení nápravných opatření v oblasti zvládání auditních a kontrolních zjištění;
- poradenská činnost v oblasti kontrol – připomínky a návrhy kontrol do plánu kontrol, pomoc s vyhodnocením kontrol, postup realizace kontrol;
- aplikace best practice, aktuálních trendů a možný rozvoj činností v této oblasti;
- metodická, procesní a dokumentační podpora v oblasti analýzy a správy rizik;
- monitoring výkonnosti SŘBI Objednatele a účinnosti bezpečnostních opatření;
- podpora při tvorbě návrhu ročního plánu budování bezpečnostního povědomí;
- podpora při tvorbě návrhů individuálních plánů vzdělávání v dané oblasti;
- podpora při vedení evidence záznamů o vzdělávání a přípravě návrhu roční zprávy o budování bezpečnostního povědomí;
- podpora pro metodiku a řízení provádění bezpečnostních testů;
- podpora při sdílení informací o kybernetických hrozbách a útocích na nadnárodních platformách;
- podpora při přípravě podkladů pro přezkoumání systému řízení bezpečnosti informací vedením organizace Objednatele;
- návrh konfigurací, implementace a správa bezpečnostních prvků;
- podpora zvyšování bezpečnostního povědomí v oblasti informační a kybernetické bezpečnosti ve vazbě na doplňkovou službu Zvyšování bezpečnostního povědomí;
- a další oblasti podpory pro SŘBI a informační a kybernetickou bezpečnost dle požadavků Objednatele.

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

5.3 Pravidelná zpráva o stavu služby dle tohoto katalogového listu

Zpráva obsahuje tyto informace:

- Období poskytování Služby KL_KC;
- Režim poskytování Služby KL_KC;
- Popis rozsahu Služby KL_KC;
- Provozovaná prostředí;
- Aktivity Služby KL_KC;
- Řízení provozu Služby KL_KC;

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

- Návrh na nápravná opatření a doporučení.

6 SLA PARAMETRY

Poskytovatel je povinen poskytovat Službu KL_KC dle Smlouvy v rozsahu definovaném objednávkou, a to v níže uvedených parametrech.

Ovlivnění chodu všech částí Služby KL_KC ze strany Objednatele (přerušení komunikace na straně Objednatele, a to úplné nebo částečné a obdobné) a z důvodů mimo působnost Poskytovatele se nezapočítává do nedostupnosti žádné z částí Služby KL_KC.

6.1 Požadovaná měsíční dostupnost Části Služby – Část 1 a Část 2 – Přístup do prostředí Nástroje

Název Služby:	**Kompetenční centrum kybernetické bezpečnosti**	
SLA parametry		
Část Služby:	**Dostupnost Služby:**	**Servisní okno pro odstávky:**
Část 1 – Administrace v Nástroji pro podporu řízení SŘBI (součást Nástroj pro řízení SŘBI)	95 %	každý čtvrtek, vždy 19:00-24:00
Část 2 – Administrativní podpora v oblasti Ochrany osobních údajů dle ZoKB (součást Nástroj pro řízení SŘBI)	95 %	každý čtvrtek, vždy 19:00-24:00

Tabulka – Přístup do prostředí Nástroje – Část 1 a Část 2

Nedostupnost Služby KL_KC – Část 1 (Administrace v Nástroji pro podporu řízení SŘBI, součást Nástroj pro řízení SŘBI) a Část 2 (Administrativní podpora v oblasti Ochrany osobních údajů dle ZoKB, součást Nástroj pro řízení SŘBI) způsobená hardwarovou nebo jinou technickou závadou se počítá od okamžiku zahájení nedostupnosti Služby KL_KC – Část 1 a Část 2 ve výše definovaném rozsahu do okamžiku obnovení poskytování. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti Služby KL_KC – Část 1 a Část 2 ve výše definovaném rozsahu, počítá se nedostupnost služby od doby jejího nahlášení.

Za nahlášení nedostupnosti služby se považuje založení odpovídajícího servisního hlášení v aplikaci Service Desk SPCSS.

Nedostupnost součástí Služby KL_KC – Zpracování zprávy o stavu Služby KL_KC dle tohoto katalogového listu určené Objednateli (předávána v měsíčním intervalu) - neovlivňuje dostupnost a kvalitu poskytované Služby KL_KC ve výše definovaném rozsahu a nemá tak vliv na plnění příslušného SLA.

6.1.1 Postup výpočtu dostupnosti Služby

Dostupnost služby se vypočítá podle následujícího vzorce:

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

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

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, mimořádné odstávky a další specifické Části Služby KL_KC.

6.1.2 Požadované lhůty pro obnovení Služby KL_KC – vybraná část části 1 a části 2

Název Služby:	**Kompetenční centrum kybernetické bezpečnosti**		
Část Služby:	**Lhůta pro obnovení služby v běžné provozní době v hodinách**		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Část 1 – Administrace v Nástroji pro podporu řízení SŘBI (součást Nástroj pro řízení SŘBI)	48	96	168
Část 2 – Administrativní podpora v oblasti Ochrany osobních údajů dle ZoKB (součást Nástroj pro řízení SŘBI)	48	96	168

Tabulka – Požadované lhůty pro obnovení Služby KL_KC – Části 1 a Část 2

Kategorizace provozních incidentů:	
Incident kategorie A	Služba KL_KC není dostupná ve svých základních a klíčových funkcích, a přitom tato funkční závada znemožňuje její užívání. Tento stav kritickým způsobem omezuje běžný provoz.
Incident kategorie B	Služba KL_KC, je ve svých funkcích degradována tak, že tento stav zásadně omezuje (Nefunkční dílčí součást v rozsahu vybrané součásti Části 1 a Část 2) její běžný provoz.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Tabulka – Kategorizace provozních incidentů

6.2 REAKČNÍ DOBY A DOBY PODPORY SLUŽBY KL_KC

Doba reakce na požadavek je počítána od zadání požadavku do aplikace Service Desk SPCSS (Poskytovatele). Za reakci je považována odpověď na požadavek. Složité a kombinované požadavky jsou rozděleny na dílčí požadavky a jsou vyřizovány sériově ve lhůtách odpovídajících každému jednotlivému požadavku. O rozdělení složitých a kombinovaných požadavků a celkové době pro vyřešení všech dílčích požadavků informuje Poskytoval Objednatele v reakci na požadavek.

Název Služby:	**Kompetenční centrum kybernetické bezpečnosti**	
SLA parametry		
Část Služby:	**Maximální doba reakce na požadavek Objednatele**	**Doba vyřešení požadavku**
Část 1 – Administrace v Nástroji pro podporu řízení SŘBI	Do 24 hodin od doby přijetí požadavku	Do 24 hodin od doby reakce na požadavek
Část 1 – Metodická podpora Objednatele	Do 24 hodin od doby přijetí požadavku	V termínu schváleném Objednatelem
Část 2 – Administrativní podpora v oblasti Ochrany osobních údajů dle ZoKB	Do 24 hodin od doby přijetí požadavku	Do 24 hodin od doby reakce na požadavek
Část 2– Zvyšování bezpečnostního povědomí	Do 24 hodin od doby přijetí požadavku	V termínu schváleném Objednatelem

Tabulka – Reakční doby a doby vyřešení požadavku

Doba reakce na požadavek Objednatele je počítána v režimu 5x8, dle kapitoly 2 – Režim poskytování služby. V případě obdržení požadavku v pracovní den, který předchází dni pracovního klidu, je reakce na požadavek odeslána následující pracovní den.

Doba vyřešení požadavku Objednatele je počítána v režimu 5x8, dle kapitoly 2 – Režim poskytování služby. V případě odeslání reakce na požadavek v pracovní den, který předchází dni pracovního klidu, je řešení požadavku zpracováno následující pracovní den – platí pro Část 1 – Administrace v Nástroji pro podporu řízení SŘBI a Část 2 - Administrativní podpora v oblasti Ochrany osobních údajů dle ZoKB. Doba řešení požadavku pro Část 1 – Metodická podpora Objednatele a Část 2 – Zvyšování bezpečnostního povědomí se řídí termínem schválení Objednatele. Ve stejném režimu jsou vyřizovány i jednorázové požadavky na administraci platformy v rámci Části 2 - Zvyšování bezpečnostního povědomí typu správa uživatelských údajů, spuštění připraveného kurzu bez potřeby úprav kurzu apod.

Maximální doba pro vyřešení požadavku v oblasti Část 1 – Administrace v Nástroji pro podporu řízení SŘBI a Část 2 – Administrativní podpora v oblasti Ochrany osobních údajů dle ZoKB platí v případě, že je

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

z požadavku zřejmé, co Objednatel požaduje a že dodal úplné podklady pro vyřešení požadavku. V opačném případě se doba vyřešení požadavku prodlužuje o dobu potřebnou k vyjasnění požadavku nebo doplnění podkladů Objednatelem.

Reakce na požadavek Objednatele v oblasti Část 1 – Metodická podpora Objednatele a Část 2 – Zvyšování bezpečnostního povědomí bude zahrnovat návrh dalšího postupu řešení včetně časového harmonogramu, náročnosti realizace a podmínky pro splnění požadavku Objednatelem, který Objednatel schválí. Na řešení požadavku budou zahájeny práce až ve chvíli schválení návrhu a harmonogramu řešení Objednatelem.

6.3 Plánované odstávky

V rámci poskytování Služby KL_KC si Poskytovatel vyhrazuje právo na plánované odstávky celého nebo částí systému z důvodu údržby jak samotného systému, tak infrastruktury a datové konektivity Poskytovatele. Poskytovatel se zavazuje plánované práce s vlivem na dostupnost Služby KL_KC soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL_KC ovlivněna co nejméně.

Plánované odstávky jsou, pokud možno, soustředěny do servisních oken, která jsou každý čtvrtek v čase 19:00 až 24:00. Ve výjimečných případech jsou odstávky Služby KL_KC realizovány i mimo tato servisní okna. Za ohlášení se považuje informování určených osob Objednatele e-mailem, a to minimálně 24 hodin před zahájením mimořádné odstávky. Doba odstávky, která byla předem řádně ohlášena, se nezapočítává do nedostupnosti Služby KL_KC. Ovlivnění chodu Služby KL_KC ze strany Objednatele se nezapočítává do nedostupnosti Služby KL_KC.

7 DOPLŇKOVÉ SLUŽBY

Doplňkové služby nemohou být poskytovány samostatně. Podmínkou pro poskytování doplňkových služeb je využití hlavní služby Kompetenční centrum kybernetické bezpečnosti. Režim poskytování doplňkových služeb je v souladu s kapitolou 2 a kapitolou 6 tohoto katalogového listu.

Volitelně může Služba KL_KC zajišťovat:

7.1 Administrativní podporu v oblasti ochrany osobních údajů dle ZoKB

- přípravu poučení osob zpracovávajících osobní údaje (přiřazení textu Objednatele do automatizované tvorby dokumentu „Poučení“);
- evidenci smluv se zpracovateli nebo jiný typ smluv s přesahem do oblasti ochrany osobních údajů;
- správu a vedení / aktualizaci Záznamů o činnostech zpracování – na základě dodaných podkladů;
- správu katalogu příjemců, právních základů, kategorií osobních údajů, šablon dokumentů např. pro nástup a výstup zaměstnance, informace k předávání osobních údajů atd. dle požadavku Objednatele.
- Služba KL_KC zahrnuje pouze administrativní podporu v oblasti Ochrany osobních údajů dle ZoKB, nezahrnuje právní služby v oblasti Ochrany osobních údajů.

7.2 Zvyšování bezpečnostního povědomí

- 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;
- vytváření tematicky zaměřených či časově omezených kurzů na základě podkladů dodaných Objednatelem;

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

- podpora procesu zvyšování bezpečnostního povědomí – přidělení kurzu určeným uživatelům, připomínky neabsolvovaných kurzů, průběžný reporting stavu a výsledků;
- aktualizace kurzů při změně vnitřních předpisů či na základě požadavku Objednatele;
- kurzy reflektují obecné informace z oblasti informační a kybernetické bezpečnosti i konkrétní nastavení politik a opatření zakotvených ve vnitřních předpisech organizace;
- znalosti absolventů nabyté v průběhu kurzů jsou ověřovány on-line testováním v průběhu či v závěru kurzů;
- vytváření testovacích úloh/zásobníku úloh, rozdělení úloh dle obtížnosti, volba způsobu řazení a výběru otázek v testu, nastavení časového limitu, počtu pokusů na úspěšné složení testů a další možnosti pro testování a klasifikaci účastníků;
- nastavení způsobu vyhodnocení a klasifikace testů absolvovaných účastníky s možností volby různých škál hodnocení;
- vystavování certifikátu jako dokladu o absolvování kurzu pro účastníky;
- uživatelská podpora – řešení požadavků typu způsob přihlášení, přidělení více pokusů na absolvování testu, prodloužení doby na absolvování kurzu apod.;
- reporting – přehled uživatelů, kteří absolvovali kurz – pro evidenci SŘBI;
- možnost vyhodnocování účinnosti plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zvyšováním bezpečnostního povědomí;
- autentizace uživatelů s využitím stávajících systémů Objednatele (např. Active Directory); systém také umožňuje import uživatelů a kurzů z externích databází a zdrojů dat (např. z formátu CSV);
- propojení s externími aplikacemi a zdroji (např. vkládání a přehrávání multimediálních souborů).
- Nedostupnost podpůrné platformy pro realizaci vzdělávání není překážkou pro poskytování doplňkové části služby Zvyšování bezpečnostního povědomí. Objednatel zadává požadavky do aplikace Service Desk SPCSS (Poskytovatele) a požadavek bude vyřešen Poskytovatelem.

8 SOUČINNOST PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY

Objednatel stanoví seznam určených osob pro plnění Služby KL_KC, tento seznam předá Poskytovateli do 5 pracovních dnů od účinnosti příslušné Objednávky. Objednatel je povinen každou změnu určených osob prokazatelně oznámit Poskytovateli.

Objednatel poskytne nezbytnou součinnost Poskytovateli při vytváření výstupů Služby KL_KC při nominacích kompetentních osob poskytujících součinnost při zpracování výstupů Služby na straně Objednatele a jeho smluvních partnerů. Zejména se jedná o nominace příslušných rolí do realizačních týmů a stanovení jejich potřebných odpovědností a kompetencí s ohledem na poskytovanou Službu KL_KC;

Objednatel bude spolupracovat s Poskytovatelem při zajištění potřebné disponibility nominovaných členů realizačních týmů pro poskytnutí součinnosti s ohledem na odsouhlasené termíny;

Objednatel bude spolupracovat s Poskytovatelem při poskytnutí všech nezbytných podkladů týkajících se obsahu zadaných výstupů Služby KL_KC.

Hlášení poruchy Služby KL_KC oznamuje Objednatel na Service Desk Poskytovatele.

Poskytovatel se zavazuje na vyžádání Objednatele sdělit členy realizačního týmu Poskytovatele, a to včetně jejich certifikace.

Služba Vstupní analýza a Realizace ověření provozu není samostatným Výstupem plnění Služby KL_KC dle kapitoly 3.2. Tyto služby mohou být realizovány na základě samostatných Objednávek, postupem dle Rámcové smlouvy.

Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

9 SMLUVNÍ POKUTY

V případě, že Poskytovatel nesplní některou ze stanovených SLA povinností, tj. stanovené dostupnosti příslušné Služby uvedené v odst. 6 tohoto katalogového listu, je Objednatel oprávněn požadovat smluvní pokutu ve výši 100 % z poměrné části příslušné měsíční Ceny za Službu bez DPH za dobu, kdy příslušná Služba nesplnila stanovené SLA.

V případě prodlení Poskytovatele s odstraněním závady příslušné Služby ve lhůtě stanovené v odst. 6 tohoto katalogového listu, má Objednatel právo uplatnit vůči Poskytovateli smluvní pokutu ve výši 100 % z poměrné části příslušné měsíční Ceny za Službu bez DPH za dobu přesahující hodnotu parametru doby vyřešení kritické závady dané Služby.

V případě prodlení Poskytovatele s dodáním Předmětu plnění specifikovaném v odst. 5.2 tohoto katalogového listu, má Objednatel právo uplatnit vůči Poskytovateli smluvní pokutu, jejíž výše a parametry budou uvedeny v konkrétní Nabídce a následné Objednávce.

10 POUŽITÉ VÝRAZY

Výraz	Popis
SPCSS	Státní pokladna Centrum sdílených služeb, s. p.
ÚKB SPCSS	Úsek Kybernetické bezpečnosti SPCSS.
KCKB	Kompetenční centrum kybernetické bezpečnosti.
Nástroj	Nástroj pro podporu řízení SŘBI.
ZoKB	Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
VoKB	Vyhláška 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).
SŘBI	Systém řízení bezpečnosti informací.
KBU	Kybernetická bezpečnostní událost je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
KBI	Kybernetický bezpečnostní incident je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

SPCSS Státní pokladna Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Rámcová smlouva o poskytování cloudových a dalších souvisejících služeb

Příloha č. 5 – Ceník Služeb kybernetické bezpečnosti

	Popis rozsahu Služby	v Kč bez DPH	DPH	v Kč včetně DPH
Služba KL_BM	Rozsah jednotek bezpečnostního monitoringu pro stanovení jednotkové ceny	v Kč bez DPH za 1 jednotku za měsíc	DPH	v Kč včetně DPH za 1 jednotku za měsíc
Bezpečnostní monitoring (jednotka - počet událostí za vteřinu)	1 - 500	1 140,57 Kč	239,52 Kč	1 380,09 Kč
	501 - 1 000	518,26 Kč	108,83 Kč	627,09 Kč
	1 001 - 2 000	358,01 Kč	75,18 Kč	433,19 Kč
	2 001 - 5 000	259,75 Kč	54,55 Kč	314,30 Kč
	5 001 - 10 000	218,57 Kč	45,90 Kč	264,47 Kč
	10 001 - 15 000	203,88 Kč	42,81 Kč	246,69 Kč
	15 001 - 20 000	198,43 Kč	41,67 Kč	240,10 Kč
	20 001 - 25 000	194,75 Kč	40,90 Kč	235,65 Kč
	25 001 - 30 000	192,93 Kč	40,52 Kč	233,45 Kč
	30 001 - 40 000	190,36 Kč	39,98 Kč	230,34 Kč
Doplňkové služby KL_BM	Rozsah Služby	v Kč bez DPH za měsíc	DPH	v Kč včetně DPH za měsíc
Bezpečnostní monitoring databází	1 ks/databáze	28 497,70 Kč	5 984,52 Kč	34 482,22 Kč
Virtuální kolektor - Bezpečnostní monitoring databází	1 ks/kolektor	11 483,46 Kč	2 411,53 Kč	13 894,99 Kč
Virtuální agregátor - Bezpečnostní monitoring databází	1 ks/agregátor	11 483,46 Kč	2 411,53 Kč	13 894,99 Kč
Virtualizace DB - Virtuální kolektor pro Bezpečnostní monitoring databází	virtualizace pro 1 kolektor (32 BB, 600 GB)	13 674,62 Kč	2 871,67 Kč	16 546,29 Kč
Virtualizace DB - Virtuální agregátor pro Bezpečnostní monitoring databází	virtualizace pro 1 agregátor (32 BB, 1 536 GB)	16 571,31 Kč	3 479,98 Kč	20 051,29 Kč
Virtuální kolektor - Bezpečnostní monitoring	1 ks/kolektor	2 105,54 Kč	442,16 Kč	2 547,70 Kč
Virtuální procesor - Bezpečnostní monitoring	1 ks/procesor	2 105,54 Kč	442,16 Kč	2 547,70 Kč
Virtualizace BM - Virtuální kolektor pro Bezpečnostní monitoring	virtualizace pro 1 kolektor (64 BB, 512 GB)	11 187,01 Kč	2 349,27 Kč	13 536,28 Kč
Virtualizace BM - Virtuální procesor pro Bezpečnostní monitoring	virtualizace pro 1 procesor (112 BB, 1 024 GB)	19 973,32 Kč	4 194,40 Kč	24 167,72 Kč
Úložný prostor	256 GB	792,28 Kč	166,38 Kč	958,66 Kč
Služba KL_VM	Rozsah Služby	v Kč bez DPH za měsíc	DPH	v Kč včetně DPH za měsíc
Vulnerability management	1 CI	355,67 Kč	74,69 Kč	430,36 Kč
Vulnerability management - engine	1 ks engine	12 628,70 Kč	2 652,03 Kč	15 280,73 Kč
Virtualizace pro nasazení 1 engine	virtualizace pro 1 ks engine (4 BB, 100 GB, správa)	5 011,29 Kč	1 052,37 Kč	6 063,66 Kč
Úložný prostor	256 GB	792,28 Kč	166,38 Kč	958,66 Kč

SPCSS
Státní pokladna
Centrum sdílených služeb
Národní plán obnovy
Financováno Evropskou unií NextGenerationEU
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Tento projekt je spolufinancován z prostředků Evropské unie z fondu Next Generation EU, Národní plán obnovy.

Služba KL_KC	Rozsah Služby	v Kč bez DPH za měsíc	DPH	v Kč včetně DPH za měsíc
Kompetenční centrum KB (jednotka - počet dokumentů)	SŘBI do správy 25 dokumentů	251 549,72 Kč	52 825,44 Kč	304 375,16 Kč
	SŘBI do správy 50 dokumentů	280 400,49 Kč	58 884,10 Kč	339 284,59 Kč
	SŘBI do správy 75 dokumentů	309 251,26 Kč	64 942,76 Kč	374 194,02 Kč
	SŘBI do správy 100 dokumentů	405 420,48 Kč	85 138,30 Kč	490 558,78 Kč
	SŘBI do správy 150 dokumentů	501 589,71 Kč	105 333,84 Kč	606 923,55 Kč
	SŘBI do správy 200 dokumentů	559 291,24 Kč	117 451,16 Kč	676 742,40 Kč
	Rozsah Služby	v Kč bez DPH za akceptované člověkodny odborných rolí	DPH	v Kč včetně DPH za akceptované člověkodny odborných rolí
	SŘBI - metodická podpora	Cena dle rozsahu a akceptace - dle sazby za 1 člověkoden uvedené v Příloze č. 1 Smlouvy		
Služba KL_PU	Rozsah jednotek pro stanovení jednotkové ceny	v Kč bez DPH za 1 jednotku za měsíc	DPH	v Kč bez DPH za 1 jednotku za měsíc
Řízení přístupu privilegovaných účtů a Session Recording (jednotka - počet souběžných uživatelů)	1 - 50	4 268,10 Kč	896,30 Kč	5 164,40 Kč
	51 - 100	2 718,40 Kč	570,86 Kč	3 289,26 Kč
	101 - 150	2 408,46 Kč	505,78 Kč	2 914,24 Kč
	151 - 200	2 275,62 Kč	477,88 Kč	2 753,50 Kč
	201 - 250	2 201,83 Kč	462,38 Kč	2 664,21 Kč
	251 - 300	2 154,87 Kč	452,52 Kč	2 607,39 Kč
Doplňkové Služby KL_PU	Rozsah Služby	v Kč bez DPH za měsíc za balíček dle rozsahu	DPH	v Kč včetně DPH za měsíc za balíček dle rozsahu
Password Management (jednotka - počet uživatelů)	balíček 25	13 066,76 Kč	2 744,02 Kč	15 810,78 Kč
	balíček 50	23 629,92 Kč	4 962,28 Kč	28 592,20 Kč
	balíček 75	32 372,27 Kč	6 798,18 Kč	39 170,45 Kč
	balíček 100	39 749,01 Kč	8 347,29 Kč	48 096,30 Kč
	balíček 125	46 075,29 Kč	9 675,81 Kč	55 751,10 Kč
	balíček 150	51 576,21 Kč	10 831,00 Kč	62 407,21 Kč
	balíček 175	56 416,85 Kč	11 847,54 Kč	68 264,39 Kč
	balíček 200	60 720,99 Kč	12 751,41 Kč	73 472,40 Kč
	balíček 225	64 583,32 Kč	13 562,50 Kč	78 145,82 Kč
	balíček 250	68 077,48 Kč	14 296,27 Kč	82 373,75 Kč
	balíček 275	71 261,57 Kč	14 964,93 Kč	86 226,50 Kč
	balíček 300	74 182,14 Kč	15 578,25 Kč	89 760,39 Kč