SPCSS
Státní pokladna
Centrum sdílených služeb

RÁMCOVÁ SMLOUVA O POSKYTOVÁNÍ SLUŽEB DATOVÉHO CENTRA

evidovaná u Objednatele pod č. SM7124-044, č.j. 123882/2024-MZV/ORIKT
evidovaná u Poskytovatele pod č. SML2024139, číslo jednací SPCSS-07085/2024
(dále jen „***Smlouva***“)

Smluvní strany:

Česká republika – Ministerstvo zahraničních věcí

se sídlem: Loretánské nám. 101/5, 118 00 Praha 1
za niž jedná: [redacted]
IČO: 45769851
DIČ: CZ45769851
bankovní spojení: [redacted]
č. účtu: [redacted]
ID DS: e4xaaxh

(dále jen „***Objednatel***“ nebo „***MZV***“)

a

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: [redacted]
IČO: 03630919
DIČ: CZ03630919
bankovní spojení: [redacted]
číslo účtu: [redacted]
ID DS: ag5uunk

(dále jen „***Poskytovatel***“ nebo „***SPCSS***“)

(dále společně také jen „***Smluvní strany***“ nebo jednotlivě „***Smluvní strana***“)

uzavřely níže uvedeného dne, měsíce a roku tuto 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 „***Zákon o zadávání veřejných zakázek***“).

I. ÚVODNÍ USTANOVENÍ

1.1 Objednatel prohlašuje, že:

1.1.1 je ústředním orgánem státní správy pro oblast zahraniční politiky, v jejímž rámci vytváří koncepci a koordinuje zahraniční rozvojovou pomoc a koordinuje vnější ekonomické vztahy, a

1.1.2 ke dni uzavření této Smlouvy naplňuje podmínky pro využití vertikální spolupráce dle § 11 odst. 1 Zákona o zadávání veřejných zakázek; 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 Smlouvy, dojde-li v průběhu trvání této Smlouvy ke změně relevantní právní úpravy;

1.1.3 splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.2 Poskytovatel prohlašuje, že:

1.2.1 je státním podnikem existujícím podle českého právního řádu; a

1.2.2 splňuje veškeré podmínky a požadavky ve Smlouvě stanovené a je oprávněn Smlouvu uzavřít a řádně plnit závazky v ní obsažené, a to i jako významný dodavatel ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „***Zákon o kybernetické bezpečnosti***“) a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání

v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), (dále jen „***Vyhláška o kybernetické bezpečnosti***“);

1.2.3 v souladu s varováním Národního úřadu pro kybernetickou a informační bezpečnost vydaným podle § 12 odst. 1 Zákona o kybernetické bezpečnosti, 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.:

1.2.3.1 nemá sídlo v Ruské federaci;

1.2.3.2 není závislý na dodávkách z území Ruské federace;

1.2.3.3 plnění dle Smlouvy nebude dodáváno prostřednictvím pobočky Poskytovatele v Ruské federaci;

1.2.3.4 plnění dle Smlouvy nemá svůj vývoj či výrobu lokalizovanou v Ruské federaci;

1.2.3.5 jeho významní dodavatelé ve smyslu § 2 písm. n) Vyhlášky o kybernetické bezpečnosti nepoužívají ICT služby či produkty závislé na dodavatelích s významným vztahem k Ruské federaci;

1.2.4 v souladu s čl. 5k 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, není:

1.2.4.1 ruským státním příslušníkem, fyzickou či právnickou osobou nebo subjektem či orgánem se sídlem v Rusku,

1.2.4.2 právnickou osobou, subjektem nebo orgánem, které jsou z více než 50 % přímo či nepřímo vlastněny některým ze subjektů uvedených v bodě 1.2.4.1 tohoto pododstavce, nebo

1.2.4.3 fyzickou nebo právnickou osobou, subjektem nebo orgánem, které jednají jménem nebo na pokyn některého ze subjektů uvedených v bodě 1.2.4.1 tohoto pododstavce nebo bodě 1.2.4.2 tohoto pododstavce,

1.2.4.4 a to včetně poddodavatelů, dodavatelů nebo subjektů, jejichž způsobilost je využívána ve smyslu Zákona o zadávání veřejných zakázek, pokud představují více než 10 % hodnoty plnění, nebo společně s nimi. Pokud v průběhu účinnosti Smlouvy dojde k nedodržení podmínek dle bodů 1.2.4.1 až 1.2.4.3 tohoto pododstavce, zavazuje se Poskytovatel bezodkladně o této skutečnosti písemně informovat Objednatele;

1.2.5 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 Smlouvy dojde k nedodržení podmínky dle věty první tohoto pododstavce, zavazuje se Poskytovatel bezodkladně o této skutečnosti písemně informovat Objednatele;

1.2.6 ve smyslu varování Národního úřadu pro kybernetickou a informační bezpečnost, vydaného podle § 12 odst. 1 Zákona o kybernetické bezpečnosti 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.

1.3 Každá ze Smluvních stran prohlašuje:

1.3.1 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 „Zákon o trestní odpovědnosti právnických osob");

1.3.2 že zavedla potřebná opatření, aby nedošlo ke spáchání trestného činu v jakékoli formě, který by jí mohl být přičten podle Zákona o trestní odpovědnosti právnických osob;

1.3.3 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;

1.3.4 že učinila nezbytná opatření k zamezení nebo odvrácení případných následků spáchaného trestného činu;

1.3.5 že z hlediska prevence trestní odpovědnosti právnických osob učinila vše, co po ní lze spravedlivě požadovat.

1.4 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, podvodu, 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.

1.5 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 1.4 tohoto článku Smlouvy a mohlo by souviset s plněním této Smlouvy nebo s jejím uzavíráním.

1.6 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 při plnění svých závazků vzniklých z této Smlouvy dodržovat, a to na vlastní náklady a odpovědnost.

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

1.8 Smlouva se uzavírá na základě výjimky z působnosti Zákona o zadávání veřejných zakázek, a to z důvodů stanovených v § 11 a/nebo v § 63 odst. 3) písm. b).

1.9 Pojmy s velkými počátečními písmeny definované ve Smlouvě či Objednávce budou mít význam, který je jim ve Smlouvě či Objednávce, vč. jejich příloh a dodatků, připisován.

II. ÚČEL A PŘEDMĚT SMLOUVY

2.1 Smlouva je uzavírána za účelem sjednání základních rámcových podmínek pro poskytování služeb Poskytovatele v oblasti IT a oblasti kybernetické bezpečnosti Objednateli. K dosažení tohoto cíle chce Objednatel využít Poskytovatelem poskytované plnění na základě jednotlivých Objednávek specifikovaných níže.

2.2 Předmětem této Smlouvy je úprava vzájemných práv a povinností Smluvních stran pro účely poskytování služeb Poskytovatele v oblasti IT a oblasti kybernetické bezpečnosti dle specifikace uvedené v odst. 2.4 tohoto článku, předmětem této Smlouvy je tak stanovení podmínek, za kterých bude docházet mezi Smluvními stranami k uzavírání objednávek (dále jen „***Objednávka***“) za podmínek dále specifikovaných v této Smlouvě.

2.3 Předmětem Smlouvy je mimo jiné také zakotvení oprávnění Objednatele vyzvat Poskytovatele

v souladu s postupem uvedeným v čl. IV. Smlouvy k uzavření Objednávek na služby specifikované v odst. 2.4 tohoto článku, a tyto Objednávky s ním následně za podmínek stanovených Smlouvou uzavřít, a dále zakotvení závazku Poskytovatele na základě výzvy Objednatele uzavřít za podmínek stanovených Smlouvou Objednávku.

2.4 Poskytovatel se v souladu s touto Smlouvou a příslušnou Objednávkou zavazuje poskytnout pro Objednatele

2.4.1 služby specifikované v jednotlivých katalogových listech v **Příloze č. 1** Smlouvy

(dále jednotlivě také jen „***Služba***“ nebo společně jen „***Služby***“);

2.4.2 Konzultace související s poskytováním Služeb dle této Smlouvy formou poskytnutí činností rolí (dále jen „***Konzultace***“). Podrobná specifikace Konzultací je uvedena v **Příloze č. 2** Smlouvy;

2.4.3 jednorázové činnosti související s poskytováním Předmětu plnění (včetně Služeb uvedených v katalogových listech v **Příloze č. 1** Smlouvy) poskytované prostřednictvím jednotlivých rolí uvedených v **Příloze č. 2 a Příloze č. 10** Smlouvy, jejímž předmětem bude dílo (např. v podobě zpracování analýzy, dokumentace, implementace požadovaného řešení, PoC, přípravy Služby apod.) (dále jen ***„Ostatní činnosti“***)

(2.4.1, 2.4.2 a 2.4.3 dále společně jako ***„Předmět plnění“***).

2.5 Poskytovatel se zavazuje poskytovat Služby v kvalitě definované v jednotlivých Service Level Agreements (dále jen „***SLA***“), přičemž SLA jednotlivých Služeb jsou definovány v **Příloze č. 1** Smlouvy v jednotlivých katalogových listech nebo jednotlivých Objednávkách Služeb.

2.6 Poskytovatel je povinen poskytnout Objednateli všechna data, která Poskytovatel shromáždil

v průběhu poskytování Služeb a na základě kterých vytvořil výstupy v rámci Služeb.

Podrobnosti o formě a způsobu předání dat stanoví Objednatel v Objednávce nebo katalogovém listu. Cena za poskytnutí těchto dat je taktéž zahrnuta v cenách uvedených v čl. VI Smlouvy

a Poskytovateli nevzniká za toto poskytnutí nárok na jakékoli jiné plnění, a to s výjimkou poskytnutí dat z cloudových platforem, které jsou součástí služeb, avšak tvoří jejich samostatnou externí část, přičemž předání dat se bude řídit příslušnou Objednávkou k realizaci Exit plánu. Poskytovatel předá data Objednateli v termínech a způsobem stanoveným v příslušné Objednávce v souladu s platnými a účinnými právními předpisy. V případě předávání dat z cloudových platforem, které tvoří samostatnou externí část, je Poskytovatel oprávněn požadovat po Objednateli úhradu nákladů stanovených poskytovatelem těchto externích cloudových služeb.

2.7 Obecné podmínky poskytování Předmětu smlouvy, stejně jako princip tvorby ceny jsou specifikovány v této Smlouvě.

2.8 Objednatel se zavazuje poskytnout Poskytovateli veškerou součinnost, nezbytnou pro řádné splnění Smlouvy ze strany Poskytovatele. Objednatel se dále zavazuje řádně provedený Předmět plnění převzít a zaplatit za ně dohodnutou cenu v souladu s platebními podmínkami uvedenými v čl. VI Smlouvy a ostatními podmínkami této Smlouvy.

2.9 Poskytovatel se zavazuje a zaručuje, že veškeré činnosti a věcná plnění, které mají být provedeny na základě této Smlouvy a Objednávek, budou provedeny řádně a v dohodnutých termínech se znalostí a péčí, které je možné očekávat od odborníků, kteří mají požadované znalosti a relevantní zkušenosti s realizací činností obdobných jako je předmět této Smlouvy. Při poskytování plnění jinou osobou má Poskytovatel odpovědnost, jako by plnil sám. Poskytovatel výslovně prohlašuje, že je s předmětem plnění této Smlouvy dostatečně obeznámen, předmět plnění této Smlouvy je vymezen dostatečně určitým způsobem a s vědomím rozsahu závazků vyplývajících z této Smlouvy Poskytovatel uzavírá tuto Smlouvu.

2.10 Poskytovatel prohlašuje, že disponuje veškerými potřebnými oprávněními pro poskytování Předmětu plnění.

2.11 Poskytovatel je při uzavírání, jakož i při plnění Objednávek povinen postupovat v souladu s touto Smlouvou a danou Objednávkou.

2.12 Poskytovatel je povinen poskytnout Objednateli veškerá licenční práva tak, aby mohl být naplněn předmět a účel této Smlouvy. Cena za poskytnutí práv dle tohoto odstavce je již zahrnuta v cenách dle čl. VI Smlouvy a Poskytovateli nevzniká za toto poskytnutí nárok na jakékoli jiné plnění.

III. DOBA A MÍSTO PLNĚNÍ

3.1 Smluvní strany sjednávají, že doba plnění příslušného Předmětu plnění bude vždy stanovena v příslušné Objednávce uzavřené dle této Smlouvy. Pro vyloučení pochybností Smluvní strany výslovně sjednávají, že účinnost každé Objednávky nastane nejdříve zveřejněním Objednávky v registru smluv 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), ve znění pozdějších předpisů (dále jen „***Zákon o registru smluv***"). Změnu termínů plnění mohou dohodnout oprávněné osoby uzavírající Objednávku.

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

IV. OBJEDNÁVKY A POSTUP JEJICH UZAVŘENÍ

4.1 Plnění z rámce sjednaného touto Smlouvou poskytuje Poskytovatel na základě Objednávek. Objednatel může uzavírat s Poskytovatelem Objednávky podle svých potřeb po celou dobu účinnosti Smlouvy, a to postupem a za podmínek stanovených tímto článkem. Objednatel se zavazuje poskytovat Poskytovateli pro plnění jednotlivých typů Služeb součinnost, tj. v rámci každé Objednávky pro danou Službu se Objednatel zavazuje před započetím s poskytováním Služby předat Poskytovateli vstupy definované v Objednávce dané Služby, a to dle specifikace uvedené v **Příloze č. 1** (v jednotlivých katalogových listech) Smlouvy. Aniž by bylo dotčeno předcházející znění, Smluvní strany uvádějí, že realizace Konzultací bude probíhat na základě jednotlivých Objednávek uzavíraných vždy do vyčerpání objednaného počtu člověkodnů uvedeného v Objednávce nebo do termínu stanoveného v Objednávce, podle toho, která ze skutečností nastane dříve. Smluvní strany dále uvádějí, že realizace Ostatních činností bude probíhat na základě jednotlivých Objednávek za účelem dokončení díla do termínu stanoveného v Objednávce.

4.2 Realizace Předmětu plnění bude probíhat na základě jednotlivých Objednávek uzavíraných vždy pro daný typ Předmětu plnění, na základě písemné výzvy Objednatele k poskytnutí dané Služby, Konzultace či Ostatních činností, zaslané prostřednictvím e-mailové zprávy Oprávněné osobě Poskytovatele (dále jen „***Výzva***"). Výzva musí obsahovat:

4.2.1 identifikační údaje Objednatele a Poskytovatele;

4.2.2 požadovaný termín zahájení a ukončení poskytování Služeb a/nebo Ostatních činností;

4.2.3 specifikaci požadované Služby a/nebo Ostatních činností včetně specifikace jejího rozsahu;

4.2.4 v případě Konzultací termín poskytování Konzultací a popis jednotlivých poptávaných rolí, případně jejich požadované certifikace;

4.2.5 v případě, že je požadovaný Předmět plnění financován či spolufinancován ze strukturálních fondů EU (dále jen „***SF EU***") název a číslo příslušného projektu SF EU (dále jen „***Projekt SF EU***"), případně další náležitosti, vyplývající z pravidel stanovených řídícím orgánem pro daný projekt, přičemž Objednatel se zavazuje Poskytovatele s danými pravidly včas seznámit;

4.2.6 podpis Oprávněné osoby Objednatele.

4.3 Poskytovatel může bez zbytečného odkladu nejpozději však do 3 (tří) pracovních dnů ode dne doručení Výzvy požádat o doplnění či upřesnění specifikace požadovaného Předmětu plnění a jejího rozsahu dle pododst. 4.2.3 tohoto článku. Požádá-li Poskytovatel o doplnění či upřesnění specifikace, staví se lhůta pro odeslání nezávazné nabídky do okamžiku zaslání řádně upravené/doplněné nové Výzvy.

4.4 Na základě Výzvy dle odst. 4.2 tohoto článku Smlouvy, a ve lhůtě maximálně 10 (deset) pracovních dnů ode dne doručení Výzvy Poskytovateli, je Poskytovatel povinen předložit Oprávněné osobě Objednatele svou nezávaznou nabídku, jejíž vzor je součástí Smlouvy jako její **Příloha č. 3** (dále jen „***Nabídka***"), nedohodnou-li se Oprávněné osoby jinak.

4.5 Nabídka bude zejména obsahovat:

4.5.1 přesnou specifikaci a rozsah Služby, která má být na základě příslušné Objednávky poskytována dle **Přílohy č. 1** (dle daného katalogového listu) Smlouvy/ přesnou specifikaci a rozsah Ostatních činností /v případě Konzultací specifikaci rolí a počet nabízených člověkodnů;

4.5.2 nabídkovou cenu stanovenou v souladu se Smlouvou, tj. dle principu stanovení ceny uvedeného vždy pro daný Předmět plnění v **Příloze č. 1**, **Příloze č. 2** a **Příloze č. 10** Smlouvy, a to případně v rozpadu na jednotlivé požadavky dle charakteru daného Předmětu plnění;

4.5.3 podrobnou specifikaci bezpečnostních podmínek, je-li to nutné;

4.5.4 harmonogram plnění Služby, Ostatních činností či Konzultací, pokud bude relevantní v rámci dané Služby či Ostatních činností;

4.5.5 akceptační kritéria, pokud budou relevantní v rámci dané Služby či Ostatních činností, přičemž nesmí být v rozporu s procesem akceptace dle čl. V Smlouvy;

4.5.6 SLA a smluvní pokuty za nedodržení SLA v případě, kdy nejsou stanoveny v jednotlivém katalogovém listu Služby;

4.5.7 členy realizačního týmu Poskytovatele, pokud bude jejich uvedení relevantní v rámci daného Předmětu plnění, včetně doložení jejich certifikace, bude-li vyžadována;

4.5.8 požadovaný termín zahájení a ukončení poskytování Služby/termín plnění Konzultací a/nebo Ostatních činností.

4.6 Nabídku Poskytovatele vypracovanou v souladu s odst. 4.4 a 4.5 tohoto článku Smlouvy Objednatel prostřednictvím Oprávněné osoby Objednatele buď akceptuje, anebo vyzve Poskytovatele k její úpravě či doplnění.

4.7 Dojde-li k akceptaci Nabídky Poskytovatele dle odst. 4.6 tohoto článku Smlouvy, předloží Poskytovatel Oprávněné osobě Objednatele návrh Objednávky, jejíž vzor je součástí Smlouvy jako její **Příloha č. 4** (dále jen „***Objednávka***"), zpracovaný dle akceptované Nabídky a dle podmínek této Smlouvy, a to nejpozději do 10 (deseti) dnů ode dne doručení akceptace Nabídky, nedohodnou-li se Oprávněné osoby Smluvních stran jinak. Objednatel může vznést k tomuto návrhu Objednávky své připomínky. Nevznese-li Objednatel k tomuto návrhu připomínky, zavazují se Smluvní strany uzavřít bez zbytečného odkladu Objednávku. Má-li Objednatel k tomuto návrhu připomínky, zavazuje se Poskytovatel s Objednatelem o těchto připomínkách jednat. Obě strany jsou při těchto jednáních povinny postupovat tak, aby došlo co nejdříve k uzavření Objednávky.

4.8 Objednávka musí vždy obsahovat alespoň následující ujednání:

4.8.1 číselné označení Objednávky;

4.8.2 označení Smluvních stran;

4.8.3 preambuli s uvedením bližšího kontextu důvodů uzavírání příslušné Objednávky;

4.8.4 předmět Objednávky s konkrétním označením, o který Předmět plnění se jedná dle této Smlouvy a dále přesnou specifikaci a rozsah Služby, která má být na základě příslušné Objednávky poskytována dle **Přílohy č. 1** a **Přílohy č. 2** Smlouvy / přesnou specifikaci

a rozsah Ostatních činností /v případě Konzultací specifikaci rolí a rovněž uvedení počtu objednaných člověkodnů;

4.8.5 vstupy pro Předmět plnění v souladu s čl. IV odst. 4.1 Smlouvy;

4.8.6 Místo plnění, pokud bude odlišné od článku 3.2 Smlouvy;

4.8.7 cenu stanovenou v souladu se Smlouvou, a to případně také v rozpadu na jednotlivé požadavky dle charakteru Předmětu plnění;

4.8.8 vymezení součinnosti Smluvních stran;

4.8.9 SLA a smluvní pokuty za nedodržení SLA v případě, kdy nejsou stanoveny v jednotlivém katalogovém listu Služby;

4.8.10 členy realizačního týmu Poskytovatele dle Nabídky, pokud bude jejich uvedení relevantní v rámci daného Předmětu plnění;

4.8.11 dobu trvání a ukončení poskytování Předmětu plnění;

4.8.12 kvalitativní a technické parametry na Ostatní činnosti;

4.8.13 harmonogram realizace, pokud bude relevantní v rámci dané Služby, Konzultace či Ostatních činností;

4.8.14 akceptační kritéria, pokud budou relevantní v rámci dané Služby či Ostatních činností, přičemž nesmí být v rozporu v procesem akceptace dle čl. V Smlouvy;

4.8.15 v případě, že je požadovaný Předmět plnění financován či spolufinancován ze strukturálních fondů EU (dále jen „***SF EU***"), název a číslo příslušného projektu SF EU (dále jen „***Projekt SF EU***"), případně další náležitosti, vyplývající z pravidel stanovených řídícím orgánem pro daný projekt, přičemž Objednatel se zavazuje Poskytovatele s danými pravidly včas seznámit;

4.8.16 podpisy Odpovědných osob ve věcech smluvních obou Smluvních stran;

4.8.17 podrobnou specifikaci bezpečnostních podmínek, je-li to nutné.

4.9 Služby budou Poskytovatelem poskytovány nepřetržitě po dobu účinnosti Objednávky. Aniž by byla dotčena předcházející věta, zavazuje se Poskytovatel poskytovat Konzultace a Ostatní činnosti v souladu s danou Objednávkou, tj. způsobem a v termínech uvedených v Objednávce.

4.10 Při plnění Objednávek je Poskytovatel povinen postupovat v souladu s touto Smlouvou a s danou Objednávkou. Na základě uzavřené Objednávky se Poskytovatel zavazuje poskytnout požadovaný Předmět plnění.

4.11 Poskytovatel se zavazuje v rámci realizace Konzultací dle každé předmětné Objednávky vést výkaz Konzultací (dle dané Objednávky). Ve výkazu Konzultací se prokazuje skutečně vynaložený čas na Konzultace s přesností na dvě desetinná místa v případě, že Konzultace nebyly poskytnuty po celý člověkoden, a to vždy s uvedením konkrétních vykonaných činností v rámci Konzultací (dále jen „***Výkaz***"). Vzor výkazu je uveden v **Příloze č. 8** Smlouvy.

V. AKCEPTACE PŘEDMĚTU PLNĚNÍ

5.1 Potvrzení o poskytnutí Služeb dle čl. II odst. 2.4 pododst. 2.4.1 v rámci všech účinných Objednávek uzavřených na základě této Smlouvy, bude realizováno formou podpisu záznamu o poskytnutí uvedených Služeb, jehož vzor je součástí **Přílohy č. 5** Smlouvy (dále jen „***Záznam***"), a to následovně:

5.1.1 Poskytovatel se zavazuje vystavit Záznam za příslušný kalendářní měsíc do 5 (pěti) pracovních dnů následujících po skončení kalendářního měsíce, ve kterém byly předmětné Služby v rámci všech účinných Objednávek poskytovány, a v této lhůtě jej předloží Objednateli.

5.1.2 Objednatel se zavazuje Záznam potvrdit a podepsat ve lhůtě 5 (pěti) pracovních dnů ode dne jeho předložení a v této lhůtě jej doručit Poskytovateli, přičemž v případě, že tak ve stanovené lhůtě neučiní, bude Záznam o poskytnutí uvedených Služeb Poskytovatelem považován za akceptovaný.

5.1.3 Sporné případy poskytnutí uvedených Služeb budou řešeny v rámci Zprávy postupem dle odst. 5.2 tohoto článku.

5.2 Hodnocení a kontrola plnění příslušných Služeb v rámci všech účinných Objednávek uzavřených na základě této Smlouvy bude probíhat vždy za uplynulý kalendářní měsíc následovně:

5.2.1 Objednatel provádí kontrolu plnění předmětných Služeb na základě zprávy o úrovni a rozsahu poskytovaných Služeb v rámci všech účinných Objednávek v příslušném období (dále jen „***Zpráva***"), přičemž vzor Zprávy je součástí **Přílohy č. 6** Smlouvy;

5.2.2 Poskytovatel se zavazuje předložit Objednateli písemnou Zprávu vždy do 10. (desátého) pracovního dne měsíce následujícího po měsíci, ve kterém byly příslušné Služby poskytovány.

5.2.3 Objednatel se zavazuje ve lhůtě 10 (deseti) pracovních dnů ode dne předložení Zprávy zpracovat ke Zprávě písemné stanovisko, kterým Zprávu akceptuje nebo ji spolu s tímto stanoviskem vrátí Poskytovateli k opravě. Nedoručí-li Objednatel písemné stanovisko ke zprávě do 10 (deseti) dnů od doručení Zprávy, považuje se Zpráva za akceptovanou bez připomínek.

5.2.4 V případě, že nebude Zpráva Objednatelem ve lhůtě dle pododst. 5.2.3 akceptována, zavazují se Smluvní strany o sporných bodech jednat. Při nesplnění podmínek stanovených touto Smlouvou a danou Objednávkou, tj. při nedodržení stanovených podmínek pro poskytování předmětných Služeb Poskytovatelem, může následně dojít

k uplatnění příslušných sankcí dle čl. XIII Smlouvy.

5.3 Na základě vyhodnocení Zprávy mohou Oprávněné osoby Smluvních stran navrhnout přijetí případné změny v úrovni poskytovaných Služeb formou změnového požadavku dle čl. VII Smlouvy.

5.4 Hodnocení, kontrola plnění a akceptace Konzultací dle **Přílohy č. 2** Smlouvy bude probíhat vždy za každý uplynulý kalendářní měsíc účinnosti předmětné Objednávky, v kterém byly Konzultace poskytovány.

5.5 Hodnocení, kontrolu plnění a akceptaci Konzultací provádějí Oprávněné osoby Smluvních stran, přičemž akceptaci plnění Konzultací na základě Výkazu, jehož vzor tvoří **Přílohu č. 8** Smlouvy, předloženého k akceptaci Poskytovatelem bude provádět Oprávněná osoba Objednatel.

5.6 Oprávněná osoba Poskytovatele se zavazuje předložit Oprávněné osobě Objednatele prostřednictvím e-mailu ke schválení Výkaz za daný kalendářní měsíc, vždy do 5. (pátého) pracovního dne kalendářního měsíce následujícího po kalendářním měsíci, v rámci kterého byly Konzultace poskytovány.

5.7 Oprávněná osoba Objednatele se zavazuje Výkaz ve lhůtě 10 (deseti) pracovních dnů ode dne doručení Výkazu svým podpisem schválit, případně do něj uvést výhrady. Poskytovatel se zavazuje vypořádat případné výhrady nejpozději do 10 (deseti) dnů od doručení podepsaného Výkazu Objednatelem a výsledek sdělit písemně prostřednictvím e-mailu Oprávněné osobě Objednatele.

Po odstranění případných výhrad sepíší Smluvní strany nový Výkaz bez výhrad.

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

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

5.8.2 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. 9** Smlouvy (dále jen ***„Akceptační protokol"***).

5.8.3 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).

5.8.4 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 nebo Akceptačního protokolu s výhradami bude vždy přílohou příslušné faktury za poskytnutí Ostatních činností.

VI. CENA A PLATEBNÍ PODMÍNKY

6.1 Poskytovatel se zavazuje poskytovat Předmět plnění dle jednotlivých Objednávek uzavíraných dle této Smlouvy s Objednatelem nejvýše za ceny uvedené v příslušné Objednávce na Předmět plnění (dále jen „***Cena Předmětu plnění***")

6.2 Ceny za Služby dle čl. II odst. 2.4 pododst. 2.4.1, jsou na základě dohody Smluvních stran stanoveny jako paušální ceny za jeden kalendářní měsíc poskytování dané Služby a jsou stanoveny na základě zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů, a to s výjimkou ceny za přípravu služby, přičemž principy stanovení každé Ceny za Službu jsou uvedeny v **Příloze č. 1**

a Příloze č. 10 Smlouvy pro daný typ Služby.

6.3 Cena za Konzultace dle čl. II odst. 2.4 pododst. 2.4.2 Smlouvy, tj. za Konzultace je stanovena dle následujícího výpočtu:

cena za jeden člověkoden (jeden člověkoden se skládá z osmi člověkohodin) pro danou roli dle Přílohy č. 2 Smlouvy * počet prokazatelně vynaložených člověkodnů na poskytování Konzultací v rámci dané role v předmětném kalendářním měsíci na základě dané Objednávky. 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 akceptovaného času skutečně stráveného na poskytování Konzultací, přičemž Poskytovatel bude účtovat čas s přesností na dvě desetinná místa, v případě, že Konzultace nebudou poskytovány s přesností po celý člověkoden.

6.4 Cena za Službu dle čl. II odst. 2.4 pododst. 2.4.3 Smlouvy, tj. za Ostatní činnosti je stanovena jako součin rozsahu poskytnutých Ostatních činností Poskytovatelem v rámci předmětné Objednávky vyjádřeného v člověkodnech v rámci dané role dle **Přílohy č. 2** Smlouvy a jednotkové ceny za člověkoden pro danou roli dle **Přílohy č. 2** Smlouvy; 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***").

6.5 Ceny za Předmět plnění stanovený na základě odst. 6.2, 6.3 a 6.4 tohoto článku se zvýší o částku odpovídající dani z přidané hodnoty (DPH) dle sazby daně platné k datu uskutečnění zdanitelného plnění.

6.6 Poskytovatel a Objednatel prohlašují, že jsou plátcem DPH.

6.7 Smluvní strany se dohodly, že celkový souhrn plnění dle této Smlouvy, tj. plnění v rámci všech uzavřených Objednávek dle této Smlouvy nesmí přesáhnout částku ve výši **500 000 000 Kč** (slovy: pět set milionů korun českých) bez DPH (dále jen „***Maximální souhrnná cena***").

6.8 Ceny dle této Smlouvy a předmětných Objednávek lze měnit pouze za podmínek stanovených touto Smlouvou nebo danou Objednávkou, přičemž nesmí překročit Maximální souhrnnou cenu dle odst. 6.7 tohoto článku Smlouvy. Současně se Smluvní strany zavazují, že v případě, kdy v průběhu plnění Objednávek uzavřených na poskytování Předmětu plnění dojde k požadavku Objednatele na změnu rozsahu poskytování jednotek daného typu Předmětu plnění v rámci dané Objednávky a v důsledku toho by mělo dojít ke změně jednotkové ceny pro daný typ Předmětu plnění, uzavřou pro daný typ Předmětu plnění novou Objednávku zahrnující i požadované změny jednotek pro daný typ Předmětu plnění, která v plném rozsahu nahradí původní Objednávku.

6.9 Ceny za Služby a Konzultace dle příslušných Objednávek budou Objednatelem hrazeny měsíčně,

a to na základě řádných daňových dokladů (faktur) vystavených Poskytovatelem zpětně za každý kalendářní měsíc poskytování Služeb a Konzultací v rámci všech platných Objednávek. Pro Služby dle čl. II odst. 2.4 pododst. 2.4.1 Smlouvy je Poskytovatel oprávněn vystavit fakturu za daný kalendářní měsíc nejdříve v den akceptace Záznamu po akceptaci Záznamu. Kopie akceptovaného Záznamu bude přílohou faktury. Pro Předmět plnění dle čl. II odst. 2.4 pododst. 2.4.2 Smlouvy,

tj. Konzultace je Poskytovatel oprávněn vystavit fakturu za daný kalendářní měsíc nejdříve v den akceptace Výkazu. Kopie akceptovaného Výkazu bude přílohou faktury. Smluvní strany se dohodly, že v případě, kdy nebudou Služby dle č. II odst. 2.4 pododst. 2.4.1 poskytovány po celý kalendářní měsíc (tj. v případě, když bude s poskytováním Služby započato v průběhu kalendářního měsíce, příp. bude poskytování Služby ukončeno v průběhu kalendářního měsíce), se Cena za Službu poměrně krátí, a to s přesností na celé dny trvání poskytování předmětné Služby. Cena za případnou přípravu Služby bude uhrazena jednorázově po oznámení Poskytovatele o zřízení Služby, a to samostatnou fakturou nebo jako samostatná položka v příslušné měsíční faktuře. Pro Předmět plnění dle čl. II odst. 2.4 pododst. 2.4.3 Smlouvy, tj. Ostatní činnosti je Poskytovatel oprávněn vystavit fakturu nejdříve v den akceptace Akceptačního protokolu bez výhrad a nebo Akceptačního protokolu s výhradami. Kopie akceptovaného Akceptačního protokolu bude přílohou faktury. Smluvní strany se dohodly, že v případě Ostatních činností lze akceptovat také dílčí plnění, pokud tak stanoví Objednávka.

6.10 Faktura musí obsahovat zejména:

6.10.1 číslo Smlouvy, popř její slovní identifikaci;

6.10.2 číslo Objednávky, příp. Objednávek, za které je fakturováno;

6.10.3 název a číslo Projektu SF EU (nebo obdobný) uvedený v Objednávce v případě, že je Předmět plnění financován či spolufinancován ze SF EU, případně další náležitosti, vyplývající z pravidel stanovených řídícím orgánem pro daný projekt, přičemž Objednatel se zavazuje Poskytovatele s danými pravidly včas seznámit;

6.10.4 specifikaci jednotlivých Služeb či Ostatních činností, které jsou fakturovány, příp. rovněž uvedení počtu člověkodnů, za které je fakturováno v případě faktury za Konzultace;

6.10.5 Cenu za Předmět plnění, příp. Ceny za Předmět plnění v rámci všech platných Objednávek, bez DPH a s DPH, sazbu DPH a výši DPH;

6.10.6 úplné bankovní spojení Poskytovatele s tím, že číslo účtu musí odpovídat číslu účtu uvedenému v záhlaví Smlouvy, tj. číslu účtu v registru plátců DPH, popř. číslu účtu oznámenému postupem dle této Smlouvy;

6.10.7 veškeré náležitosti dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „***Zákon o DPH***"), v případě, že se jedná o daňový doklad;

6.10.8 náležitosti obchodní listiny uvedené v § 435 odst. 1 Občanského zákoníku.

6.11 Faktury jsou splatné ve lhůtě 30 (třiceti) kalendářních dnů ode dne řádného doručení Objednateli. Pro vyloučení pochybností Smluvní strany uvádějí, že datem uskutečnění zdanitelného plnění pro Služby dle čl. II odst. 2.4 pododst. 2.4.1, je poslední den kalendářního měsíce, ve kterém byly Služby poskytovány, pro Předmět Plnění dle čl. II odst. 2.4 pododst. 2.4.2 Smlouvy (Konzultace) je datem uskutečnění zdanitelného plnění datum akceptace Výkazu Objednatelem a pro Předmět Plnění dle čl. II odst. 2.4 pododst. 2.4.3 Smlouvy (Ostatní činnosti) je datem uskutečnění zdanitelného plnění datum akceptace Akceptačního protokolu Objednatelem bez výhrad a nebo Akceptačního protokolu s výhradami.

6.12 Poskytovatel bude faktury doručovat prostřednictvím datové schránky Objednatele nebo na e-mail [redacted].

6.13 Objednatel je oprávněn ve lhůtě 15 (patnácti) dnů ode dne doručení faktury fakturu vrátit Poskytovateli, aniž by došlo k prodlení s její úhradou, obsahuje-li nesprávné náležitosti nebo údaje, chybí-li na faktuře některá z náležitostí nebo údajů nebo chybí-li některá z příloh, popř. je-li faktura jinak neoprávněně účtovaná. Poskytovatel je povinen v případě vrácení faktury dle předcházející věty fakturu opravit nebo vyhotovit fakturu novou. Ode dne doručení opravené, příp. nové faktury běží Objednateli nová lhůta splatnosti v délce 30 (třiceti) kalendářních dnů.

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

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

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

6.17 Poskytovatel je oprávněn zvýšit každou z Cen za Předmět plnění dle této 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.

6.18 Poskytovatel je oprávněn zvýšit každou z Cen za Předmět plnění 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 Předmět plnění nesnižuje. Poskytovatel je v každém roce oprávněn zvýšit každou Cenu za Předmět plnění nejvýše o 10 %; to platí i v případě, že Míra inflace za předcházející kalendářní rok bude vyšší.

6.19 Nebude-li oznámení o zvýšení každé z Cen za Předmět plnění doručeno Objednateli do 31. března daného kalendářního roku, právo na uplatnění zvýšení Ceny za Předmět plnění v daném kalendářním roce zanikne. Pro vyloučení pochybností Smluvní strany sjednávají, že za účelem zvýšení kterékoliv z Cen za Předmět plnění dle odst. 6.1 až odst. 6.4 tohoto článku není nutné uzavírat dodatek ke Smlouvě.

6.20 Změna sazby DPH nebude považována za změnu této Smlouvy nebo změnu Ceny za Předmět plnění, která podléhá sjednání dodatku ke Smlouvě (viz článek XVIII. odst. 6.17 a 6.18, též článek VII. odst. 7.3); DPH bude v takovém případě účtována ke Ceně za Předmět plnění automaticky v souladu se změnou příslušného zákona.

VII. ZMĚNOVÉ ŘÍZENÍ

7.1 Kterákoliv ze Smluvních stran je oprávněna písemně navrhnout změny Předmětu plnění

a parametrů jejich poskytování v rámci příslušné Objednávky, a to prostřednictvím požadavku zaslaného e-mailem Oprávněné osobě příslušné Smluvní strany (dále jen „***Změnový požadavek***"). Žádná ze Smluvních stran není povinna navrhované změny akceptovat.

7.2 Poskytovatel se zavazuje provést hodnocení dopadů navrhovaných změn Předmětu plnění z hlediska vhodnosti, termínů plnění, součinnosti Smluvních stran a ceny dle příslušné Objednávky. Poskytovatel se zavazuje provést hodnocení bez zbytečného odkladu, nejpozději do 10 (deseti) pracovních dnů ode dne doručení Změnového požadavku, není-li Smluvními stranami dohodnuto jinak.

7.3 Smluvní strany se zavazují za účelem potvrzení změn dle tohoto článku uzavřít dodatek ke Smlouvě nebo dané Objednávce, kterým budou provedené změny do Smlouvy nebo dané Objednávky promítnuty, není-li ve Smlouvě výslovně sjednáno jinak. V závislosti na takovém dodatku může být upraven požadovaný rozsah Předmětu plnění, termíny Předmětu plnění, cena Předmětu plnění, platební podmínky, součinnost Objednatele atd.

7.4 Obě Smluvní strany se zavazují případné změny či doplňky této Smlouvy či Objednávky činit písemně vzestupně číslovanými dodatky, které jsou nedílnou součástí této Smlouvy či Objednávky.

VIII. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

8.1 Poskytovatel se zavazuje:

8.1.1 poskytovat Služby v kvalitě definované v jednotlivých SLA, které jsou stanoveny v **Příloze č. 1** (v jednotlivých katalogových listech) Smlouvy anebo jednotlivých Objednávkách Služby;

8.1.2 poskytovat Předmět plnění řádně a včas bez faktických a právních vad;

8.1.3 postupovat při realizaci Předmětu plnění 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 s Předmětem plnění, které Objednatel Poskytovateli poskytne, nebo s pokyny jím pověřených osob;

8.1.4 bez zbytečného odkladu oznámit Objednateli veškeré skutečnosti, které mohou mít vliv na povahu nebo na podmínky poskytování Předmětu plnění dle Smlouvy a Objednávek;

8.1.5 informovat bezodkladně Objednatele o všech okolnostech důležitých pro řádné a včasné plnění Smlouvy a Objednávek;

8.1.6 poskytnout Objednateli veškerou nezbytnou součinnost k naplnění účelu Smlouvy i všech Objednávek na jejím základě uzavřených;

8.1.7 nakládat se všemi věcmi, dokumenty a dalšími písemnostmi, které mu byly Objednatelem svěřeny za účelem plnění této Smlouvy a Objednávek (dále jen „***Podklady***"), s péčí řádného hospodáře a chránit je před poškozením a zneužitím. Objednatel zůstává vlastníkem Podkladů poskytnutých Poskytovateli za účelem plnění této Smlouvy a Objednávek. Poskytovatel je oprávněn s Podklady nakládat pouze v souladu s podmínkami této Smlouvy a Objednávek. Poskytovatel není oprávněn k jinému nakládání a užití Podkladů bez předchozího písemného souhlasu Objednatele. Všechny Podklady, včetně případných kopií, je povinen chránit před nepovolanými osobami. Poskytovatel odpovídá za škodu způsobenou ztrátou a zneužitím Podkladů dle tohoto odstavce v souladu s čl. XI Smlouvy. Poskytovatel se zavazuje vrátit Objednateli veškeré Podklady, které mu byly Objednatelem svěřeny pro účely plnění Smlouvy, nejpozději do 5 (pěti) pracovních dnů od ukončení platnosti Objednávky uzavřené na základě této Smlouvy, nedohodnou-li se Smluvní strany jinak;

8.1.8 Poskytovatel tímto prohlašuje, že je pojištěn z titulu odpovědnosti za způsobenou škodu v souvislosti s poskytováním Předmětu plnění Objednateli, příp. třetí osobě, a to na pojistné plnění ve výši minimálně 200 000 000 Kč (slovy: dvě stě milionů korun českých), s tím, že toto pojistné plnění neklesne pod uvedenou hranici po celou dobu plnění závazků podle této Smlouvy.

8.1.9 Poskytovatel předloží Objednateli nejpozději v den uzavření Smlouvy kopii pojistné smlouvy nebo pojistného certifikátu. Poskytovatel je povinen udržovat platnou pojistnou smlouvu v požadované výši po celou dobu plnění dle této Smlouvy. Poskytovatel je povinen předat kopii aktuální pojistné smlouvy nebo pojistného certifikátu Objednateli kdykoliv na vyžádání Objednatele, a to bez zbytečného odkladu, nejpozději však do 10 (deseti) pracovních dnů od doručení písemné žádosti Objednatele.

8.2 Objednatel se zavazuje:

8.2.1 poskytovat Poskytovateli úplné, pravdivé a včasné informace potřebné k řádnému a včasnému poskytování Předmětu plnění;

8.2.2 poskytovat Poskytovateli součinnost potřebnou pro řádné a včasné realizování Předmětu plnění, kterou je od něho Poskytovatel jako osoba, která disponuje kapacitami

a odbornými znalostmi, které jsou nezbytné pro realizaci Předmětu plnění s odbornou péčí, oprávněna požadovat;

8.2.3 zaplatit za řádně a včas poskytnutý Předmět plnění nebo jejich části cenu dle příslušné Objednávky.

8.3 Poskytovatel se zavazuje poskytnout Objednateli potřebnou součinnost při výkonu finanční kontroly dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů a dále potřebnou součinnost oprávněným kontrolním orgánům při výkonu kontroly týkající se realizovaného Projektu SF EU.

8.4 Poskytovatel se zavazuje dodržovat relevantní ustanovení Zákona o kybernetické bezpečnosti a Vyhlášky o kybernetické bezpečnosti dle charakteru Předmětu plnění popsaných v **Příloze č. 1** Smlouvy.

8.5 Poskytovatel bere na vědomí, že poskytování Předmětu plnění dle Smlouvy může souviset

s provozem prvku kritické informační infrastruktury (dále jen „***KII***"). Objednatel a Poskytovatel je v jejich rámci vázán Zákonem o kybernetické bezpečnosti a Vyhláškou o kybernetické bezpečnosti, jakož i vnitřními předpisy Objednatele, které obdržel dle 8.6 Smlouvy.

8.6 Vnitřní předpisy Objednatele, související s KII, předá Objednatel Poskytovateli v elektronické podobě na základě oboustranně podepsaného předávacího protokolu, který obsahuje seznam předávané dokumentace, a to bezodkladně po nabytí účinnosti Smlouvy. Objednatel se zavazuje vždy bezodkladně informovat Poskytovatele o jakékoliv změně vnitřních předpisů uvedených v předchozí větě a současně s tím Poskytovateli vždy předat aktuální znění těchto vnitřních předpisů, a to postupem dle předcházející věty. Poskytovatel, jako významný dodavatel ve smyslu Zákona o kybernetické bezpečnosti a Vyhlášky o kybernetické bezpečnosti, je povinen při všech činnostech souvisejících s plněním Smlouvy brát na tuto skutečnost zřetel a dodržovat ustanovení Zákona o kybernetické bezpečnosti a Vyhlášky o kybernetické bezpečnosti a současně dodržovat bezpečnostní opatření ve formě organizačních a technických opatření, která budou vydávána příslušnými orgány Objednatele, a postupovat v souladu s předanými vnitřními předpisy Objednatele.

8.7 Poskytovatel se zavazuje během poskytování předmětu plnění dostatečně zabezpečit veškeré případné zpracování a přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost.

8.8 Poskytovatel je srozuměn s pravidelným prováděním hodnocení rizik, kontrolou a auditem zavedených bezpečnostních opatření ze strany Objednatele v souvislosti s poskytovaným předmětem plnění. Kontrola nebo audit mohou být provedeny v prostorách Poskytovatele nebo jeho poddodavatele a Poskytovatel má povinnost tyto kontroly a audity Objednateli či pověřené osobě Objednatele umožnit či možnost jejich provedení v prostorách poddodavatele zajistit, přispět k nim a poskytnout Objednateli či Objednatelem pověřené osobě k jejich provedení maximální možnou součinnost, kterou lze po Poskytovateli rozumně požadovat. Počet a frekvence kontrol ani auditů nejsou nijak omezeny.

8.9 Poskytovatel se během poskytování Předmětu plnění pro Objednatele zavazuje Objednatele informovat o:

8.9.1 kybernetických bezpečnostních incidentech souvisejících s předmětem plnění, a to bez zbytečného odkladu;

8.9.2 způsobu řízení rizik, zbytkových rizicích souvisejících s předmětem plnění a bez zbytečného odkladu také o změnách ve způsobu řízení rizik;

8.9.3 významné změně ovládání Poskytovatele nebo jeho poddodavatele podle zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů (dále jen „***Zákon o obchodních korporacích***“), a to nejpozději do 3 (tří) pracovních dnů od uskutečnění této změny;

8.9.4 změně vlastnictví zásadních aktiv, využívaných Poskytovatelem k předmětu plnění, a změně oprávnění nakládat s těmito aktivy, a to nejpozději do 3 (tří) pracovních dnů od uskutečnění této změny.

8.9.5 změně členů realizačního týmu. Objednatel/osoba oprávněná uzavřít Objednávku si vyhrazuje právo odsouhlasit změnu složení realizačního týmu. Nevyjádří-li Objednatel/osoba oprávněná uzavřít Objednávku nesouhlas se změnou realizačního týmu do 10 (deseti) dnů od data doručení oznámení, považuje se nový realizační tým za odsouhlasený. Tato změna nepodléhá sjednání dodatku ke Smlouvě.

IX. PODDODAVATELÉ

9.1 Poskytovatel se zavazuje poskytovat Předmět plnění dle této Smlouvy a Objednávek sám nebo prostřednictvím poddodavatelů. V případě, že Poskytovatel bude poskytovat Předmět plnění prostřednictvím poddodavatele, zavazuje se o tomto záměru informovat Objednatele již ve své Nabídce, a to včetně sdělení, kterou část plnění pro něj v rámci plnění Objednávky daný poddodavatel bude poskytovat. Poskytovatel se zavazuje zajistit, že případným využitím poddodavatelů nedojde k porušení Zákona o zadávání veřejných zakázek, zejména ustanovení § 11.

9.2 Zadání provedení části Předmětu plnění poddodavateli Poskytovatelem nezbavuje Poskytovatele jeho výlučné odpovědnosti za řádné provedení Předmětu plnění vůči Objednateli. Poskytovatel odpovídá Objednateli za plnění Předmětu plnění, 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. Poskytovatel se zavazuje smluvně zavázat své poddodavatele k dodržování ujednání mezi Objednatelem jako povinnou osobou ve smyslu Vyhlášky o kybernetické bezpečnosti a Poskytovatelem v plném rozsahu, přičemž tato ujednání nebudou v rozporu s požadavky Objednatele jako povinné osoby na dodavatele. Stanoví-li smlouva nebo Objednávka povinnosti ve vztahu k členům týmů Poskytovatele, vztahují se obdobně i na členy realizačního poddodavatele.

X. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

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

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

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

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

XI. NÁHRADA ÚJMY

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

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

11.3 Smluvní strany se výslovně dohodly, že celková výše všech nároků na náhradu újmy, vzniklých na základě nebo v souvislosti s touto Smlouvou, resp. jednotlivými Objednávkami jedné Smluvní straně, se omezuje částkou ve výši 200 000 000,00 Kč (slovy: dvě stě milionů korun českých). Ustanovení § 2898 Občanského zákoníku není tímto ujednáním dotčeno, tj. uvedené omezení se neuplatní u újmy způsobené člověku na jeho přirozených právech, anebo způsobené úmyslně či hrubou nedbalostí.

11.4 Náhrada újmy je splatná ve lhůtě 30 (třiceti) od doručení písemné výzvy oprávněné Smluvní strany Smluvní straně povinné z náhrady újmy.

11.5 Po dobu zásahu vyšší moci a po dobu nezbytnou k odstranění těchto zásahů nebo vlivem skutečností, při nichž nelze spravedlivě po Poskytovateli požadovat plnění provedené řádně a včas, Poskytovatel není v prodlení s plněním své smluvní povinnosti. Termín plnění se posunuje

o nezbytnou dobu, dokud tato překážka vyšší moci nepomine. O takové skutečnosti je Poskytovatel povinen v přiměřené době Objednatele informovat a sdělit mu předpokládaný náhradní termín plnění. Za vyšší moc se považuje mimořádná nepředvídatelná a neodvratitelná událost, která nastala nezávisle na vůli Poskytovatele, které nelze zabránit ani při vynaložení veškerého možného úsilí, zejména např. přírodní katastrofa, živelná pohroma, teroristický útok, válka, revoluce, stávka, povstání, vojenská akce.

XII. ODPOVĚDNOST ZA VADY

12.1 Poskytovatel je povinen poskytovat Předmět plnění v souladu s požadavky Objednatele a při dodržení povinností sjednaných v této Smlouvě a dané Objednávce. Objednatel je povinen řádně poskytnutý Předmět plnění převzít a zaplatit za ně cenu v souladu s touto Smlouvou.

12.2 Poruší-li Poskytovatel povinnosti stanovené v odst. 12.1 tohoto článku, jedná se o vadné plnění.

12.3 Poskytovatel odpovídá za to, že poskytování Předmětu plnění bude v souladu s touto Smlouvou, Objednávkou, jakož i povinnostmi stanovenými právními předpisy.

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

XIII. SMLUVNÍ POKUTY

13.1 V případě nedodržení termínů uvedených v harmonogramu dle dané Objednávky, pokud byl v rámci dané Objednávky harmonogram sjednán, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 0,5 % (půl procenta) ceny konkrétního plnění, ke kterému se prodlení vztahuje, případně z měsíční ceny Služby při nedodržení termínu zahájení Služby, a to za každý i započatý kalendářní den prodlení.

13.2 V případě prodlení Poskytovatele s povinností mít po celou dobu trvání Smlouvy uzavřenou pojistnou smlouvu dle čl. VIII odst. 8.1 pododst. 8.1.8 Smlouvy, má Objednatel právo uplatnit vůči Poskytovateli smluvní pokutu ve výši 10 000,00 Kč (slovy: deset tisíc korun českých), a to za každý započatý kalendářní den prodlení.

13.3 V případě, že některá ze Smluvních stran poruší některou z povinností dle čl. XVIII odst. 18.5 této Smlouvy, je druhá Smluvní strana oprávněna požadovat smluvní pokutu ve výši 100 000,00 Kč (slovy: jedno sto tisíc korun českých), a to za každý jednotlivý případ porušení.

13.4 V případě, že Poskytovatel nesplní některou ze stanovených SLA povinností, tj. stanovené dostupnosti příslušné Služby v katalogovém listu v **Příloze č. 1** Smlouvy, je Objednatel oprávněn požadovat smluvní pokutu ve výši stanovené v katalogovém listu příslušné Služby dle Přílohy č. 1 Smlouvy či smluvní pokutu stanovenou v příslušné Objednávce v případě, že katalogový list příslušné Služby SLA a smluvní pokutu nestanoví. Smluvní strany se dohodly, že v případě rozporu SLA a smluvních pokut stanovených katalogovým listem a Objednávkou, má přednost znění Objednávky.

13.5 V případě, že Poskytovatel nepředá Objednateli data a práva v souladu s čl. II odst. 2.6, je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 5 000,00 Kč (slovy: pět tisíc korun českých), a to za každý i započatý den prodlení.

13.6 V případě, že Poskytovatel nepředá Objednateli aktualizovaný Exit plán v termínu dle čl. XVI. odst. 16.4 Smlouvy, je povinen Poskytovatel uhradit Objednateli smluvní pokutu ve výši 1 000,00 Kč (slovy: jeden tisíc korun českých) za každý i započatý den prodlení.

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

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

13.9 Smluvní strany se výslovně dohodly, že celková výše všech nároků na smluvní pokuty vzniklých na základě nebo v souvislosti s touto Smlouvou, resp. jednotlivými Objednávkami jedné Smluvní straně se omezuje pro jednotlivé Služby uvedené v katalogových listech dle **Přílohy č. 1** Smlouvy částkou stanovenou v jednotlivých katalogových listech v Příloze č. 1 Smlouvy. Celková výše všech nároků na smluvní pokuty vzniklých na základě nebo v souvislosti s touto Smlouvou je omezena 50 % celkové výše Ceny za veškerá plnění dle uzavřených Objednávek dle této Smlouvy.

13.10 Zaplacení smluvní pokuty nezbavuje Smluvní stranu povinnosti splnit závazek utvrzený smluvní pokutou a nezbavuje nároku na náhradu újmy způsobené Smluvní straně ve výši stanovené v odst. 11.4 Smlouvy, ani nároku na odstoupení od Smlouvy.

XIV. PŘECHOD VLASTNICTVÍ A LICENČNÍ UJEDNÁNÍ

14.1 Pro případ, že výsledkem činnosti Poskytovatele nebo jeho poddodavatelů dle této Smlouvy je dílo, které naplňuje znaky díla chráněného dle § 2 zákona č. 121/2000 Sb., o právu autorském,

o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „***Autorský zákon***“) (to vše dále jen „***Autorské dílo***“):

14.1.1 Poskytovatel prohlašuje, že je oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k Autorskému dílu a že má souhlas autorů k uzavření následujících licenčních ujednání; toto prohlášení zahrnuje i taková práva autorů, která by vytvořením Autorského díla teprve vznikla;

14.1.2 Poskytovatel poskytuje Objednateli (nabyvateli licence) oprávnění ke všem v úvahu přicházejícím způsobům užití Autorského díla a bez jakéhokoliv omezení, a to zejména pokud jde o územní, časový nebo množstevní rozsah užití;

14.1.3 Smluvní strany se výslovně dohodly, že cena za poskytnutí této licence Poskytovatelem je již zahrnuta v ceně za poskytnutí Předmětu plnění, pokud není v Objednávce stanoveno jinak;

14.1.4 Poskytovatel poskytuje tuto licenci Objednateli (nabyvateli licence) jako výhradní, s tím, že Poskytovatel je oprávněn Autorské dílo sám užít pouze se souhlasem Objednatele, přičemž Objednatel nesmí souhlas odepřít bez uvedení relevantních důvodů, které bezodkladně sdělí Poskytovateli.

14.1.5 Objednatel (nabyvatel licence) není povinen licenci využít;

14.1.6 Objednatel (nabyvatel licence) je oprávněn bez dalšího práva tvořícího součást licence zcela nebo zčásti jako podlicenci poskytnout třetí osobě;

14.1.7 Objednatel (nabyvatel licence) je oprávněn upravit či jinak měnit Autorské dílo, jeho název nebo označení autorů, stejně jako spojit Autorské dílo s jiným dílem nebo zařadit Autorské dílo do díla souborného, a to přímo nebo prostřednictvím třetích osob;

14.1.8 ustanovení § 2370 a § 2378 Občanského zákoníku se nepoužijí.

14.2 Poskytovatel tímto prohlašuje, že pokud v souvislosti s plněním na základě této Smlouvy vytvořil databáze, zřídil je pro Objednatele jako pro pořizovatele databáze dle § 89 Autorského zákona

a Objednateli tak svědčí všechna práva na vytěžování nebo na zužitkování celého obsahu databáze nebo její kvalitativně nebo kvantitativně podstatné části a právo udělit jinému oprávnění k výkonu tohoto práva. Objednatel je oprávněn databázi měnit a doplňovat bez souhlasu a vědomí Poskytovatele. Změnou databáze se ale nerozumí jakékoliv úpravy dat nasbíraných v průběhu provádění díla.

14.2.1 V případě, že by se z jakéhokoliv důvodu stal pořizovatelem databáze Poskytovatel, Poskytovatel touto Smlouvou převádí veškerá práva k databázi na Objednatele a Objednatel tato práva přijímá.

14.2.2 Stejně tak v případě, že Poskytovateli vznikla na základě této Smlouvy zvláštní práva pořizovatele databáze ve smyslu § 88 a násl. Autorského zákona, Poskytovatel touto Smlouvou veškerá tato práva převádí dle § 90 odst. 5 Autorského zákona na Objednatele a Objednatel tato zvláštní práva pořizovatele databáze přijímá.

14.2.3 Smluvní strany se výslovně dohodly, že odměna za převod veškerých práv k databázi, včetně zvláštních práv pořizovatele databáze, je již zahrnuta v Cenách za Předmět plnění podle čl. VI Smlouvy.

14.3 V případě, že součástí plnění Poskytovatele podle této Smlouvy jsou movité věci (např. nosiče médií), které se mají stát vlastnictvím Objednatele, nabývá Objednatel vlastnické právo k těmto věcem dnem jejich protokolárního předání a převzetí Objednatelem.

14.4 Veškerá oprávnění dle výše uvedeného přechází na Objednatele okamžikem akceptace příslušné části Ostatních činností dle předmětné Objednávky, není-li Smluvními stranami stanoveno jinak.

XV. OCHRANA INFORMACÍ SMLUVNÍCH STRAN

15.1 Smluvní strany berou na vědomí, že vzhledem k tomu, že s plněním této Smlouvy je spojeno zpracování osobních údajů pracovníků Objednatele a případně rovněž dodavatelů Objednatele – podnikajících fyzických osob, které poskytují Objednateli v rámci pracovněprávních a obchodních vztahů (dále jen „***Osobní údaje***“) ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „***Obecné nařízení GDPR***“), je pro účely této Smlouvy Objednatel v postavení správce Osobních údajů (pro účely odst. XV.1 a XV.2 Smlouvy dále jen „***Správce***“) a Poskytovatel

v postavení zpracovatele Osobních údajů (pro účely odst. 15.1 a 15.2 Smlouvy dále jen „***Zpracovatel***“), přičemž Zpracovatel a Správce se zavazují za účelem plnění Smlouvy uzavřít samostatnou písemnou smlouvu o zpracování osobních údajů reflektující povinnosti dle Obecného nařízení GDPR, zákona č. 110/2019 Sb., o zpracování osobních údajů jakožto prováděcího předpisu k Obecnému nařízení GDPR a příslušných právních předpisů.

15.2 Smluvní strany se dohodly, že cena za zpracování Osobních údajů na základě této Smlouvy, je vždy zahrnuta v ceně za danou část Předmětu plnění dle čl. VI Smlouvy, které se zpracování Osobních údajů týká, přičemž Zpracovatel nemá nárok na náhradu nákladů spojených s plněním tohoto článku VI Smlouvy.

XVI. DOBA TRVÁNÍ A UKONČENÍ SMLOUVY

16.1 Tato Smlouva se uzavírá na dobu neurčitou, a to od okamžiku účinnosti Smlouvy, tj. od okamžiku uveřejnění Smlouvy v registru smluv v souladu se Zákonem o registru smluv na dobu neurčitou nebo do okamžiku, kdy součet vyfakturovaných cen za Předmět plnění dosáhne Maximální souhrnné ceny (viz článek VI odst.6.7) Pro vyloučení pochybností Smluvní strany stanoví, že nedojde k akceptaci Objednávek, jejíž cena plnění by přesáhla Maximální souhrnné ceny dle článku VI odst. 6.7 Smlouvy.

16.2 Smlouva, resp. jednotlivé Objednávky mohou být ukončeny dohodou Smluvních stran v písemné formě, přičemž účinky ukončení účinnosti nastanou k okamžiku stanovenému v takovéto dohodě. Nebude-li takovýto okamžik dohodou stanoven, pak tyto účinky nastanou ke dni uveřejnění takové dohody v registru smluv dle Zákona o registru smluv.

16.3 Platnost nebo účinnost Smlouvy není nijak závislá na platnosti nebo účinnosti Objednávek a zároveň platnost a účinnost Objednávek uzavřených do konce účinnosti Smlouvy není nijak závislá na platnosti a účinnosti Smlouvy.

16.4 Každá ze Smluvních stran je oprávněna Smlouvu a každou jednotlivou Objednávku vypovědět, a to i bez udání důvodu a včetně těch Objednávek, které jsou uzavřené na dobu určitou. Výpovědní doba Smlouvy činí 12 (dvanáct) měsíců a počíná běžet prvním (1,) dnem měsíce následujícího po měsíci, ve kterém bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé Smluvní straně. Výpovědní doba každé Objednávky činí 6 (šest) měsíců a počíná běžet prvním (1.) dnem měsíce následujícího po měsíci, ve kterém bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé Smluvní straně, není-li v Objednávce sjednáno jinak. Poskytovatel se zavazuje v případě podání výpovědi jednotlivé Objednávky předat Objednateli aktualizovaný Exit plán požadovaný dle článku 16.11 Smlouvy, a to do 20 (dvaceti) pracovních dnů od doručení výpovědi.

16.5 Smlouva a jednotlivé Objednávky mohou zaniknout odstoupením příslušné Smluvní strany, nastanou-li okolnosti předvídané § 2002 Občanského zákoníku (podstatné porušení povinnosti).

16.6 Za podstatné porušení povinnosti Poskytovatelem dle odst. 16.5 tohoto článku se považuje zejména:

16.6.1 prodlení s plněním dle termínů uvedených v Objednávkách zaviněné Poskytovatelem,

a které Poskytovatel nedokázal napravit ani do 15 (patnácti) kalendářních dnů po obdržení písemného oznámení Objednatele, ačkoli měl pro svoji činnost k dispozici všechny potřebné podklady a součinnost Objednatele,

16.6.2 neplnění, neúplné či jinak vadné plnění či dílčí plnění, včetně vadného plnění spočívajícího ve vadách právních, které Poskytovatel nedokázal napravit ani do 15 (patnácti) kalendářních dnů po obdržení písemného oznámení Objednatele,

16.6.3 poskytování Předmětu plnění dle Objednávky je bezdůvodně pozastaveno po dobu více než 20 (dvacet) kalendářních dnů.

16.7 Objednatel je dále oprávněn bez jakýchkoliv sankcí vůči své osobě od Smlouvy, resp. dané Objednávky odstoupit v případě, že:

16.7.1 Poskytovatel pozbude oprávnění vyžadované právními předpisy k činnostem, k jejichž provádění je Poskytovatel povinen dle Smlouvy;

16.7.2 Poskytovatel poruší závazek mít po dobu trvání této Smlouvy pojištění z titulu odpovědnosti za způsobenou škodu uvedený v čl. VIII této Smlouvy;

16.7.3 na návrh Poskytovatele bude zahájeno insolvenční řízení podle zákona č. 182/2006 Sb.,

o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (dále jen „***Insolvenční zákon***"), jehož předmětem bude úpadek nebo hrozící úpadek Poskytovatele;

16.7.4 bude zahájeno insolvenční řízení podle Insolvenčního zákona, jehož předmětem bude úpadek nebo hrozící úpadek Poskytovatele a současně bude insolvenčním soudem vydáno rozhodnutí o úpadku Poskytovatele;

16.7.5 bude zahájeno insolvenční řízení podle Insolvenčního zákona, jehož předmětem bude úpadek nebo hrozící úpadek Poskytovatele a současně bude insolvenčním soudem nařízeno předběžné opatření podle § 113 Insolvenčního zákona;

16.7.6 Poskytovatel vstoupí do likvidace;

16.7.7 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), ve znění pozdějších předpisů, či ekvivalentní postavení. Nastane-li případ dle předcházející věty, je Poskytovatel povinen informovat o této skutečnosti Objednatele písemně do 2 (dvou) dnů od jejího vzniku s uvedením bližších údajů, které by Objednatel mohl v této souvislosti potřebovat pro své rozhodnutí o odstoupení od Smlouvy.

16.8 Odstoupením se závazek založený touto Smlouvou, příp. danou Objednávkou zrušuje pouze ohledně nesplněného zbytku plnění od okamžiku neplnění závazku. Smluvní strany si jsou povinny vyrovnat dosavadní vzájemné závazky ze Smlouvy, příp. Objednávky, a to bez zbytečného odkladu, nejpozději však do 30 (třiceti) dnů od doručení oznámení Smluvní strany o odstoupení od 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 Smlouvy nedotčeny.

16.9 Poskytovatel je oprávněn od Smlouvy, resp. jednotlivých Objednávek odstoupit zejména v případě, že Objednatel bude v prodlení s úhradou svých splatných peněžitých závazků vyplývajících z této Smlouvy po dobu delší než 30 (třicet) kalendářních dnů a dále v případě, že Poskytovateli nebude Objednatelem opakovaně (nejméně 2x) poskytována součinnost v souladu s touto Smlouvou, a to ani přes písemnou výzvu Poskytovatele k nápravě.

16.10 Odstoupení od Smlouvy, jakož i Objednávky musí být písemné, jinak nemá právní účinky. Odstoupení je účinné ode dne, kdy bylo doručeno druhé Smluvní straně.

16.11 Poskytovatel se zavazuje vyhotovit ke každé jednotlivé Objednávce exit plán, který bude obsahovat výčet činností provozního a dokumentačního charakteru, souvisejících s převedením předmětu

a rozsahu Předmětu plnění dle dané Objednávky (dále jen „***Exit plán***"). Pro vyloučení pochybností Smluvní strany stanoví, že samotná realizace Exit plánu může být ze strany Poskytovatele provedena pouze na základě samostatné Objednávky postupem dle čl. IV této Smlouvy, či případně prostřednictvím změnového řízení analogicky postupem dle čl. VII Smlouvy. Cena za samostatnou Objednávku na realizaci Exit plánu bude stanovena dle Předmětu plnění uvedených v **Příloze č. 1 a 2** této Smlouvy.

16.12 Ukončením 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. XV Smlouvy, práva z odpovědnosti za vady, licenční ujednání ani další ujednání, z jejichž povahy vyplývá, že mají zavazovat Smluvní strany i po zániku účinnosti této Smlouvy nebo Objednávky.

XVII. OZNÁMENÍ A KOMUNIKACE

17.1 Jakékoliv úkony směřující k ukončení této Smlouvy nebo Objednávek musí být doručeny příslušné Smluvní straně datovou schránkou nebo formou doporučeného dopisu, nebylo-li možné doručit prostřednictvím datové schránky. Oznámení nebo jiná sdělení podle této Smlouvy nebo Objednávek se budou považovat za řádně učiněná, pokud budou učiněna písemně v českém jazyce a doručena, osobně, elektronickou poštou s připojeným zaručeným elektronickým podpisem, prostřednictvím datové schránky a nebude-li možné doručit výše uvedenými způsoby, pak kurýrem či poštou 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 ve Smlouvě jinak:

17.1.1 Objednatel:

Název: Česká republika – Ministerstvo zahraničních věcí

Adresa: Loretánské náměstí. 101/5, 118 00 Praha 1

K rukám: jméno Oprávněné osoby Objednatele

Datová schránka: e4xaaxh

17.1.2 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

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

17.3 Smluvní strany se dohodly na určení oprávněné osoby za každou Smluvní stranu (dále jen „***Oprávněná osoba***"). Oprávněné osoby jsou oprávněné ke všem jednáním týkajícím se této Smlouvy a Objednávek, není-li ve Smlouvě nebo Objednávce stanoveno jinak, s výjimkou změn nebo zrušení Smlouvy a změn nebo zrušení Objednávek. Oprávněné osoby jsou uvedeny v **Příloze č. 7** této Smlouvy.

17.4 Ke změně nebo ukončení Smlouvy, k uzavření, změně nebo ukončení Objednávky je za Objednatele oprávněna vrchní ředitelka Sekce informačních a komunikačních technologií (SIKT)

a dále osoby pověřené vrchní ředitelkou Sekce informačních a komunikačních technologií.

K uzavření, změně nebo ukončení Objednávky jsou za Objednatele oprávněny také Oprávněné osoby uvedené v **Příloze č. 7** této Smlouvy. Ke změně nebo ukončení Smlouvy, k uzavření, změně nebo ukončení Objednávky 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.

17.5 Jakékoliv změny kontaktních údajů a Oprávněných osob je příslušná Smluvní strana oprávněna provádět jednostranně a je povinna tyto změny neprodleně písemně oznámit druhé Smluvní straně. V případě změny Oprávněných osob není třeba uzavírat dodatek Smlouvy.

XVIII. ZÁVĚREČNÁ USTANOVENÍ

18.1 Obě Smluvní strany souhlasí s tím, že podepsaná Smlouva (včetně příloh) a Objednávky (včetně 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 Smlouvu a Objednávky v souladu se Zákonem o registru smluv uveřejní v registru smluv.

18.2 Tato Smlouva a Objednávky se řídí Občanským zákoníkem a dalšími příslušnými právními předpisy České republiky, není-li ve Smlouvě stanoveno jinak.

18.3 Stane-li se kterékoliv ustanovení této Smlouvy nebo Objednávky neplatným, neúčinným nebo nevykonatelným, zůstává platnost, účinnost a vykonatelnost ostatních ustanovení této Smlouvy

a Objednávek nedotčena, nevyplývá-li z povahy daného ustanovení, obsahu Smlouvy nebo Objednávky, nebo okolnosti, za nichž bylo toto ustanovení vytvořeno, že toto ustanovení nelze oddělit od ostatního obsahu 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.

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

18.5 Smluvní strany nejsou oprávněny bez předchozího písemného souhlasu druhé Smluvní strany postoupit Smlouvu jakož i Objednávky, jednotlivý závazek ze Smlouvy či Objednávek ani pohledávky vzniklé v souvislosti s touto Smlouvou nebo Objednávkami na třetí osoby, ani učinit jakékoliv právní jednání, v jehož důsledku by došlo k převodu nebo přechodu práv či povinností vyplývajících z této Smlouvy, jakož i Objednávek.

18.6 Změny nebo doplňky této Smlouvy včetně příloh a změny nebo doplňky Objednávek včetně příloh musejí být vyhotoveny písemně formou dodatku, datovány a podepsány oběma Smluvními stranami s podpisy Odpovědných osob pro věci smluvní obou Smluvních stran na jedné písemnosti, ledaže Smlouva či Objednávka v konkrétním případě stanoví jinak. Pro vyloučení pochybností Smluvní strany uvádějí, že ke změně bankovního spojení včetně čísla bankovního účtu Smluvních stran může dojít pouze písemným dodatkem ke Smlouvě.

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

18.8 Smluvní strany se dohodly, že v rámci této Smlouvy a Objednávek vylučují aplikaci § 557 Občanského zákoníku.

18.9 Tato Smlouva představuje úplnou dohodu mezi Smluvními stranami, která nahrazuje veškeré předchozí ujednání a závazky vztahující se k předmětu plnění této Smlouvy.

18.10 Smlouva nabývá platnosti dnem podpisu oběma Smluvními stranami a účinnosti dnem uveřejnění Smlouvy v registru smluv dle Zákona o registru smluv.

18.11 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.

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

18.13 Součástí této Smlouvy jsou tyto přílohy:

Příloha č. 1: Katalog služeb
KL01 Bezpečnostní monitoring
KL02 Analýza rizik

KL03 Analýza rizik předmětu veřejné zakázky
KL04 Penetrační testy
KL05 Konzultace v oblasti informační a kybernetické bezpečnosti
KL06 Vulnerability management
KL07 Kompetenční centrum kybernetické bezpečnosti
KL08 Správa privilegovaných účtů
KL09 Služby IaaS – Landing zóna pro provoz IS Objednatele
KL10 Služby PaaS pro IS s provozní podporou 8x5
KL11 Služby PaaS pro IS s provozní podporou 24x7

Příloha č. 2: Popis odborných rolí a jejich cena
Příloha č. 3: Vzor Nabídky
Příloha č. 4: Vzor Objednávky
4.1: Vzor Objednávky Služby
4.2: Vzor Objednávky Konzultace
4.3: Vzor Objednávky Ostatní činnosti
Příloha č. 5: Vzor Záznamu
Příloha č. 6: Vzor Zprávy
Příloha č. 7: Oprávněné osoby
Příloha č. 8: Vzor Výkazu
Příloha č. 9: Vzor Akceptačního protokolu
Příloha č. 10: Ceník služeb kybernetické bezpečnosti

Za Objednatele:

V Praze dne dle el. podpisu

[redacted]

Česká republika – Ministerstvo zahraničních věcí

Za Poskytovatele:

V Praze dne dle el. podpisu

[redacted]

Státní pokladna Centrum sdílených služeb, s. p.

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 1 – Katalog služeb

Seznam katalogových listů			
Označení	**Název**	**Termíny poskytování Služby**	
		zahájení	**ukončení**
KL01	Bezpečnostní monitoring	V souladu s konkrétní Objednávkou	V souladu s konkrétní Objednávkou
KL02	Analýza rizik		
KL03	Analýza rizik předmětu veřejné zakázky		
KL04	Penetrační testy		
KL05	Konzultace v oblasti informační a kybernetické bezpečnosti		
KL06	Vulnerability management		
KL07	Kompetenční centrum kybernetické bezpečnosti		
KL08	Správa privilegovaných účtů		
KL09	Služby IaaS – Landing zóna pro provoz IS Objednatele		
KL10	Služby PaaS pro IS s provozní podporou 8x5		
KL11	Služby PaaS pro IS s provozní podporou 24x7		

KATALOGOVÝ LIST č. 01

Název služby	Bezpečnostní monitoring

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Bezpečnostní monitoring (dále jen **„Služba KL01"**) je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL01.

Název milníku	Termín splnění milníku
Zahájení poskytování Služby KL01	Na základě Objednávky/Smlouvy
Ukončení poskytování Služby KL01	Na základě Objednávky/Smlouvy

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba KL01 bude poskytována v režimu, dle popisu v tabulce:

Režim poskytování Služby KL01	Doba poskytování Služby KL01
Standardní provozní doba	Nepřetržitě (24x7)

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 Vstupy

Vstupy pro Službu KL01 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 KL01 jsou:

- Poskytování Služby KL01;
- 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 KL01 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 KL01 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 KL01 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 KL01 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 KL01, 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 KL01.

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 KL01, poskytováno vždy)	
☒	Sběr logů
☒	Zpracování logů
☒	Monitorování NetFlow
☒	Proces zvládání kybernetických bezpečnostních incidentů (Incident management)
Část 2 - Ostatní součásti služby Bezpečnostní monitoring (nedílné součásti KL01, poskytováno vždy)	
☒	Uživatelská behaviorální analýza
☒	Přístup do prostředí nástroje SIEM v rozsahu Služby KL01
☒	Zpracování zprávy o stavu Služby KL01 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
☐	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 KL01 je realizována v rozsahu definovaných aktiv Objednatele. Archivované informace slouží pro forenzní analýzu ve všech sledovaných souvislostech.

V rámci Služby KL01 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. KL01 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 KL01 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 KL01, nebo využití odpovídajících Doplňkových služeb specifikovaných na základě Vstupní analýzy dle kapitoly 3.1).

- § 23 Detekce kybernetických bezpečnostních událostí

  Služba KL01 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.

- § 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí

  V prostředí Objednatele lze Službu KL01 využít pro sběr bezpečnostních událostí a jejich vyhodnocování. Služba KL01 poskytuje informace určeným bezpečnostním rolím v organizaci, čímž omezuje případy nesprávného vyhodnocení události a zajišťuje včasné varování.

- § 31 Kategorizace kybernetických bezpečnostních incidentů

  Služba KL01 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 KL01 nezahrnuje organizační opatření SŘBI Objednatele. Součástí Služby KL01 není tvorba politik, vyjma dokumentace dle kapitoly 3 tohoto katalogového listu.

5 POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL01

Předmětem Služby KL01 je nepřetržitý bezpečnostní monitoring v režimu 24x7 definovaných aktiv Objednatele.

Typy záznamů, se kterými Služba KL01 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 KL01. Podmínkou pro splnění tohoto opatření je realizace samostatné Služby Log management SPCSS, která není předmětem tohoto KL01 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 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 KL01.

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 KL01

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.

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 KL01;
- Režim poskytování Služby KL01;
- Popis rozsahu Služby KL01;
- Monitorovaná prostředí;
- Rozsah bezpečnostního dohledu;
- Detekce, sběr a vyhodnocování kybernetických bezpečnostních událostí;
- Stav dokumentace (aktualizace dokumentace dle kapitoly 3.2);
- Řízení provozu služeb;
- Řešení a stav BH (Bezpečnostní hlášení), KBU, KBI za uplynulé období a návrhy na nápravná opatření;
- Aktivity Služeb Bezpečnostního dohledu – seznam řešených offense;
- TOP 10 kategorií uplatněných pravidel na firewallu směrem z internetu;
- TOP 10 druhů komunikace zablokovaných z internetu;
- TOP 10 zablokovaných IP adres;
- TOP 10 cílových portů, na které byla zablokovaná komunikace;
- TOP 10 zablokovaných aktivit na firewallu;
- Návrh na nápravná opatření.

6 SLA PARAMETRY

Poskytovatel je povinen poskytovat Službu KL01 dle Smlouvy pro vybrané aktiva Objednatele v souladu s jednotlivými níže uvedenými kvalitativními parametry Služby pro její jednotlivé části.

Ovlivnění chodu všech částí Služby KL01 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 KL01.

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 KL01 – 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 KL01 – 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 KL01 – 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 KL01 – Část 2 - Uživatelská behaviorální analýza, Přístup do prostředí nástroje SIEM v rozsahu Služby KL01, Zpracování zprávy o stavu Služby KL01 dle tohoto katalogového listu určené Objednateli (předávána v měsíčním intervalu) - neovlivňuje dostupnost a kvalitu poskytované Služby KL01 – Část 1, Část 3 a Část 4 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:

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

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 KL01.

6.1.2 Požadované lhůty pro obnovení Služby KL01 – 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 KL01 – vybraná část Části 1, Část 3 a Část 4

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 KL01 – 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 KL01

Název Služby:	**Bezpečnostní monitoring**	
SLA parametry		
Část Služby:	Dostupnost Služby:	Servisní okno pro odstávky:
Část 2 – Přístup do prostředí nástroje SIEM v rozsahu Služby KL01	95 %	každý čtvrtek, vždy 19:00-24:00

Tabulka – Přístup do prostředí nástroje SIEM v rozsahu Služby KL01

Nedostupnost Služby KL01 – Část 2 (Přístup do prostředí nástroje SIEM v rozsahu Služby KL01) způsobená hardwarovou nebo jinou technickou závadou se počítá od okamžiku zahájení nedostupnosti Služby KL01 – Část 2 ve výše definovaném rozsahu do okamžiku obnovení poskytování. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti Služby KL01 – 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 KL01 Část 2 – Přístup do prostředí nástroje SIEM v rozsahu Služby KL01 ze strany Objednatele (přerušení komunikace na straně Objednatele, a to úplné nebo částečné a obdobné) se nezapočítává do nedostupnosti žádné z částí Služby KL01 Část 2 – Přístup do prostředí nástroje SIEM v rozsahu Služby KL01.

6.4 Plánované odstávky

V rámci poskytování Služby KL01 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 KL01 soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL01 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 KL01 ohlašovány a realizovány i mimo tato servisní okna. Doba odstávky, která byla předem řádně ohlášena se nezapočítává do nedostupnosti Služby KL01. 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

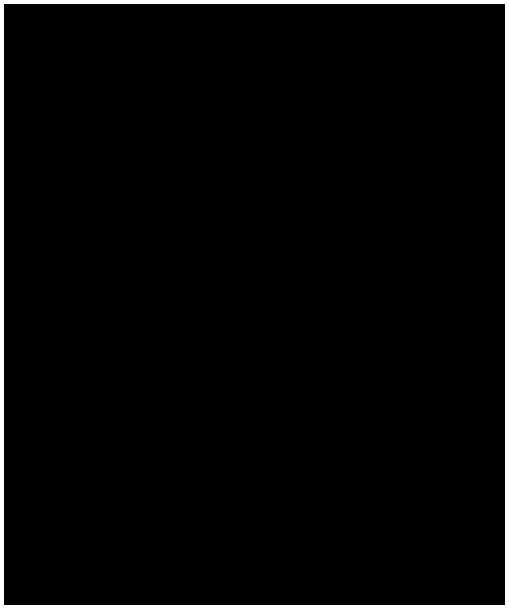
Doplňková služba Bezpečnostní monitoring databází pomáhá se zabezpečením citlivých dat v prostředí databází a datových skladů. Bezpečnostní monitoring databází se skládá ze dvou částí – kolektor (jedná se o kolektor speciálně určený pro monitoring databází) a nástroj pro analýzu a ochranu dat v databázích. 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 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 KL01 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.

Doporučení pro využití Virtuálního kolektoru databází v rámci architektury řešení poskytované Služby KL01 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.

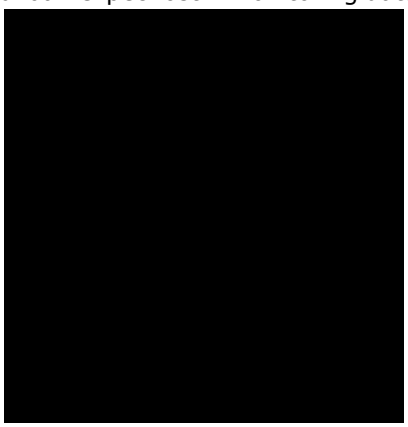
Požadovaný rozsah zdrojů virtualizace (vCPU, vRAM, HDD) je specifikován na základě Vstupní analýzy dle kapitoly 3.1.

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 KL01 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 KL01 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 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 KL01 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);
- 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;
- 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.
- 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.

9 PRINCIP STANOVENÍ CENY

Cena bude stanovena v souladu s článkem 2, odstavcem 2.4 Smlouvy a následně uvedena v konkrétní Nabídce a navazující Objednávce. To vše na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy pro následné poskytování Služby KL01.

V rámci Vstupní analýzy bude stanoveno množství jednotek pro zajištění řádného poskytování Služby KL01. Výsledná cena Služby KL01 se stanoví jako součin množství požadovaných rolí a jednotek a jejich jednotkové ceny uvedené v Příloze č. 2 a č.10 Smlouvy.

Vstupní analýza bude zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování odpovídajícího plnění.

Realizace Vstupní analýzy je povinným vstupem pro řádné stanovení ceny Služby KL01, kdy je rozhodné naplnění zpracování dílčího plnění dle výše zmíněné Rámcové smlouvy, a to:

- zpracování dokumentu „Závěrečná zpráva analýzy řešení bezpečnostního monitoringu v rozsahu informačního systému Objednatele".

Realizace ověření provozu bude zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování odpovídajícího p lnění.

Vstupem a povinnou podmínkou pro Realizaci ověření provozu je dokument „Závěrečná zpráva analýzy řešení bezpečnostního monitoringu v rozsahu informačního systému Objednatele" zpracovaný dle Vstupní analýzy, dle kapitoly 3.1.

Realizace ověření provozu je povinným vstupem pro řádné stanovení ceny Služby KL01.

Služba Vstupní analýza a Realizace ověření provozu není samostatným Výstupem plnění Služby KL01 dle kapitoly 3.2. Tyto služby mohou být realizovány na základě samostatné objednávky dílčích částí Služby KL01 a KL05 (Konzultace).

10 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 110 % 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 110 % 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.

11 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 (SOC)	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: • 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 je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého

Výraz	Popis
(VIS)	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 síť	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.
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.

Výraz	Popis
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.

KATALOGOVÝ LIST č. 02

Název služby	Analýza rizik

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby.

Název milníku	Termín splnění milníku
Zahájení poskytování služby	Na základě Objednávky
Ukončení poskytování služby	Na základě Objednávky

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba Analýza rizik bude poskytována v režimu, dle popisu v tabulce:

Režim poskytování služby	Doba poskytování Služby
Standardní provozní doba služby	Služba v rozsahu a kvalitě vyžádané objednávkou

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 Vstupy

Vstupy pro službu jsou:

- Relevantní dokumentace Objednatele
- Interview s respondenty na straně Objednatele
- Případné předchozí analýzy rizik

3.2 Výstupy

Výstupy služby jsou dokumenty:

- Zpráva o hodnocení aktiv a rizik
- Plán zvládání rizik (pouze pro systémy VIS nebo KII)
- Prohlášení o aplikovatelnosti (pouze pro systémy VIS nebo KII)
- Doplňkové soubory (hodnocení aktiv, seznam rizik, metodika analýzy rizik)

4 POPIS SLUŽBY

Služba analýzy rizik spočívá v provedení analýzy rizik v určeném rozsahu, dle zvolené metodiky a s využitím příslušných nástrojů. Výstupy služby jsou v souladu s vybranými povinnostmi vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VoKB"). Činnosti, které jsou prováděny během poskytování služby Analýza rizik, obsahují: identifikaci, evidenci aktiv a garantů aktiv, hodnocení aktiv, identifikaci relevantních hrozeb a zranitelností a zpracování povinných dokumentů.

Časové intervaly, ve kterých se Analýza rizik provádí:

Systém kritické informační infrastruktury *(KII)* - minimálně 1x za rok

Systém významného informačního systému *(VIS)* - minimálně 1x za 3 roky

Při zásadních změnách v systému podle §11 VoKB (realizace je pak provedena na základě změnového požadavku (Request for Change)).

Standardní nabídkou je pravidelná aktualizace analýzy rizik. Analýza rizik prováděná na základě zásadní změny systému není součástí standardní nabídky a její realizace je možná na základě dohody smluvních stran.

Oblasti obsažené ve službě Analýza rizik / součásti dodávky služby

Interview s garanty primárních aktiv a jejich ohodnocení.

Interview s garanty podpůrných aktiv a jejich ohodnocení.

Doplnění vazeb mezi podpůrnými a primárními aktivy.

Analýza hrozeb a zranitelností – hodnocení rizik.

Vypracování výstupní dokumentace dle VoKB (Zpráva o hodnocení aktiv a rizik, Plán zvládání rizik, Prohlášení o aplikovatelnosti), pokud se jedná o KII nebo VIS. Pokud se o KII nebo VIS nejedná, zpracovává se pouze Zpráva o hodnocení aktiv a rizik.

5 PROCES REALIZACE ANALÝZY RIZIK

V rámci realizace Analýzy rizik se postupuje podle zvolené metodiky. Stručný popis procesu je uveden níže.

5.1 Interview

Jedná se o konzultaci na bázi řízeného rozhovoru, jejíž první část se zaměřuje na identifikování rozsahu služeb a stanovení primárních aktiv (zpravidla služby nebo informace), a zároveň i jejich ohodnocení (důležitost daného aktiva a také jeho důvěrnost, dostupnost a integrita). Druhým důležitým výstupem je identifikování garantů podpůrných aktiv.

Druhá část interview se poté zaměřuje na garanty podpůrných aktiv, s nimiž je veden rozhovor na podobné bázi, jako s garanty primárních aktiv. Cílem je vytvoření přehledu všech podpůrných aktiv (a jejich případný rozpad až na úroveň IP adresy a jejich fyzického umístění) a ohodnocení z hlediska váhy vlivu na primární aktivum, které je daným podpůrných aktivem ovlivňováno (hodnotí se z hlediska váhy na dostupnost, důvěrnost a integritu primárního aktiva).

5.2 Analýza hrozeb

Dalším krokem je identifikace hrozeb a kvantifikace hrozeb. Hrozbou rozumíme jakoukoliv událost, která může způsobit narušení důvěrnosti, integrity a dostupnosti aktiva. Tato fáze se také nazývá analýza hrozeb,

při které vycházíme ze seznamu obecných hrozeb uvedených ve VoKB doplněných o specifické hrozby pro informační systém nebo pro organizaci objednatele.

5.3 Analýza zranitelností

V tomto kroku dochází k identifikaci a kvantifikaci všech slabých míst na úrovni fyzické, logické a administrativní bezpečnosti.

5.4 Hodnocení rizik

Ve chvíli, kdy známe hodnotu aktiv, pravděpodobnost hrozeb a míru zranitelnosti, dochází k hodnocení rizik.

5.5 Zpracování výstupní dokumentace

Výstupem Služby pro KII nebo VIS je zpracovaná dokumentace dle VoKB, konkrétně se jedná o:

- Zpráva o hodnocení aktiv a rizik,
- Plán zvládání rizik,
- Prohlášení o aplikovatelnosti.

Akceptace výstupní dokumentace probíhá formou akceptačního protokolu potvrzeným ze strany objednatele dle podmínek stanovených ve smlouvě. Po předání výstupní dokumentace přechází odpovědnost za jejich vydání a realizaci opatření na obědnatele, který následně vůči dozorovým orgánům vystupuje jako autor analýzy rizik, příslušné dokumentace a jako odpovědná osoba za realizaci příslušných opatření ve smyslu povinností dle VoKB.

6 PŘEDPOKLADY PRO ZAJIŠTĚNÍ 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 relevantní dokumentaci k jednotlivým IS.

7 ZÁKAZNICKÁ PODPORA

Objednatel využívá k řešení svých provozních a technických požadavků jednotné kontaktní místo, kterým je Service desk. Předmětem činnosti zákaznické podpory není provádění změnových požadavků.

8 PRINCIP STANOVENÍ CENY

Cena bude stanovena v souladu s článkem 2, odstavcem 2.4 Smlouvy a následně uvedena v konkrétní Nabídce a navazující Objednávce. To vše na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy pro následné poskytování Služby KL02.

V rámci Vstupní analýzy bude stanoveno množství jednotek pro zajištění řádného poskytování Služby KL02. Výsledná cena Služby KL02 se stanoví jako součin množství požadovaných jednotek a rolí a jejich jednotkové ceny uvedené v Příloze č.2 a Příloze č. 10 Smlouvy.

9 10 SMLUVNÍ POKUTY

V případě prodlení Poskytovatele s dodáním Předmětu plnění specifikovaném v 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
OCKB – SPCSS	Odbor Centra Kybernetické Bezpečnosti ve společnosti SPCSS, s.p.
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.
Aktivum (asset)	Cokoliv hmotného i nehmotného, co má pro nás nějakou hodnotu. Vlivem působením hrozeb, se hodnota aktiv zmenšuje. Např. hardware, software, autorská práva, informace, veškerá data na počítačích a serverech, apod.

KATALOGOVÝ LIST č. 03

Název služby	Analýza rizik předmětu veřejné zakázky

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby.

Název milníku	Termín splnění milníku
Zahájení poskytování služby	Na základě Objednávky
Ukončení poskytování služby	Na základě Objednávky

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba Analýza rizik předmětu veřejné zakázky bude poskytována v režimu, dle popisu v tabulce:

Režim poskytování služby	Doba poskytování Služby
Standardní provozní doba služby	Služba v rozsahu a kvalitě vyžádané objednávkou

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 Vstupy

Vstupy pro službu jsou:

- Relevantní dokumentace zákazníka
- Interview s respondenty na straně zákazníka
- Finální zadávací dokumentace veřejné zakázky

3.2 Výstupy

Výstupy služby jsou dokumenty:

- Dokument – Metodika analýzy rizik
- Dokument – Analýza rizik předmětu veřejné zakázky
- Doplňkové soubory (nástroj pro Analýzu rizik předmětu veřejné zakázky)

4 POPIS SLUŽBY

Služba obsahuje tvorbu Metodiky analýzy rizik předmětu veřejné zakázky a provedení analýzy rizik předmětu veřejné zakázky dle této Metodiky.

4.1 Popis služby Tvorby Metodiky analýzy rizik předmětu veřejné zakázky

Účelem dokumentu je popis Metodiky hodnocení rizik předmětu veřejné zakázky, která bude využita k dosažení souladu s požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (dále také „ZoKB") a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále také „VoKB"). Především pak dle §8 VoKB, č.2 písmeno a) v rámci veřejné zakázky a před uzavřením smlouvy provádí hodnocení rizik souvisejících s plněním předmětu veřejné zakázky přiměřeně podle přílohy č. 2 k této vyhlášce.

Metodika je navržena tak, aby splňovala veškeré požadavky ZoKB, VoKB a byla vyhotovena v souladu s obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti.

1.1.1 Podklady a spolupráce

Podmínkou pro řádné poskytování služby je, aby zákazník akceptovaný Dokument metodiky hodnocení rizik předmětu veřejné zakázky vydal v rámci interního řízení vydávání interních předpisů.

1.1.2 Výstup služby

Výstupem služby je dokument Metodika analýzy rizik předmětu veřejné zakázky uzpůsobena pro prostředí zákazníka.

4.2 Popis služby Analýzy rizik předmětu veřejné zakázky

Analýza rizik předmětu veřejné zakázky zahrnuje následující činnosti:

a) identifikace aktiv;

b) ohodnocení aktiv;

c) identifikace a ohodnocení hrozeb a zranitelností;

d) ohodnocení rizik dopadu hrozeb na aktiva;

e) určení a schválení přijatelných rizik;

f) návrh na způsob zvládání rizik;

g) závěrečné doporučení.

1.1.3 Podklady a spolupráce

Pro vytvoření analýzy rizik je nutná spolupráce s objednatelem při všech krocích analýzy rizik. Objednatel musí zajistit plnou součinnost dotčených osob, především pak garantů jednotlivých dotčených aktiv a garanta veřejné zakázky.

1.1.4 Výstupy analýzy

Výstupem procesu analýzy rizik (Metodika analýzy rizik předmětu veřejné zakázky) je zpracování vstupů objednatele, za účelem vytvoření dokumentu Hodnocení rizik předmětu veřejné zakázky.

Pro vyloučení pochybností Zadavatel a Dodavatel výslovně uvádějí a souhlasí s tím, že výstup Dodavatele má výlučně doporučující charakter, tj. Dodavatel nenese odpovědnost za jakékoliv možné dopady citovaného výstupu na veřejnou zakázku, resp. průběh zadávacího řízení veřejné zakázky.

5 PŘEDPOKLADY PRO ZAJIŠTĚNÍ 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 relevantní dokumentaci k jednotlivým veřejným zakázkám.

6 PRINCIP STANOVENÍ CENY

Cena bude stanovena v souladu s článkem 2, odstavcem 2.4 Smlouvy a následně uvedena v konkrétní Nabídce a navazující Objednávce. To vše na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy pro následné poskytování Služby KL03.

V rámci Vstupní analýza bude stanoveno množství jednotek pro zajištění řádného poskytování Služby KL03. Výsledná cena Služby KL03 se stanoví jako součin množství požadovaných rolí a jejich jednotkové ceny uvedené v Příloze č.2 Smlouvy.

7 SMLUVNÍ POKUTY

V případě prodlení Poskytovatele s dodáním Předmětu plnění specifikovaném v 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.

8 POUŽITÉ VÝRAZY

Výraz	Popis
Aktivum (asset)	Cokoliv hmotného i nehmotného, co má pro nás nějakou hodnotu. Vlivem působením hrozeb, se hodnota aktiv zmenšuje. Např. hardware, software, autorská práva, informace, veškerá data na počítačích a serverech, apod.
Garant zakázky	Garant aktiv, která jsou v procesu analýzy rizik předmětem veřejné zakázky, je zároveň garantem veřejné zakázky, případně za sebe musí navrhnout zástupce, který přebírá jeho odpovědnost a pro účely analýzy rizik předmětu veřejné zakázky se stane garantem aktiv.
Hrozba	Potencionální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva.
Zranitelnost	Slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

KATALOGOVÝ LIST č. 04

Název služby	Penetrační testy

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby.

Název milníku	Termín splnění milníku
Zahájení poskytování služby	Na základě Objednávky
Ukončení poskytování služby	Na základě Objednávky

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba Penetrační testy bude poskytována v režimu, dle popisu v tabulce:

Režim poskytování služby	Doba poskytování Služby
Standardní provozní doba služby	Služba v rozsahu a kvalitě vyžádané objednávkou

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 Vstupy

Vstupy pro službu jsou:

- Vybavení pracovníka Objednatele příslušnými kompetencemi
- Stanovení cílů penetračního testování
- Dodržování časového harmonogramu
  Poskytnutí nezbytné součinnosti

3.2 Výstupy

Výstupy služby jsou dokumenty:

- Detailní plán služby
- Report výsledků

4 POPIS SLUŽBY

Služba Penetrační testy zjišťuje, do jaké míry je konkrétní systém odolný proti útoku, kde jsou jeho slabá místa a jak je nejlépe odstranit. Tato služba je také prováděna za účelem zjištění slabin v zabezpečení infrastruktury organizace, konfiguračních chyb a bezpečnostních mezer.

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

Provádění penetračních testů informačního a komunikačního systému se zaměřením na důležitá aktiva je povinné podle Zákona č. 181/2014 Sb., o kybernetické bezpečnosti, resp. §25 odst.1 prováděcí vyhlášky č.82/2018 před jejich uvedením do provozu (KII i VIS povinně) a na základě výsledku analýzy rizik v souvislosti s významnou změnou informačního a komunikačního systému.

Aktivní testování se provádí zásadně s písemným souhlasem Objednatele a dalších osob, kterých by se mohlo testování nějak dotknout. Před započetím vlastního testování je nutné stanovit jasné podmínky testování, tedy určení času, cílů testu (adresy, domény, emaily, osoby).

Tabulka 1 – Definice rozsahu služby

Zvolené typy penetračních testů (viz 5.1.1)		**Rozsah testu**
☐	Externí penetrační testy	
☐	Interní penetrační testy	
☐	Sociální penetrační testy	
Služba je zaměřena na oblasti (viz 5.1.2)		
☐	Penetrační test sítě	☐ Základní ☐ Detailní
☐	Penetrační test Wi-Fi sítě	☐ Základní ☐ Detailní
☐	Penetrační test aplikací	☐ Základní ☐ Detailní
☐	Penetrační test webu/portálů	☐ Základní ☐ Detailní
☐	Penetrační test zaměřený na uživatele a hesla	☐ Základní ☐ Detailní
☐	Penetrační test mobilních zařízení	☐ Základní ☐ Detailní
☐	Penetrační test pracovních stanic	☐ Základní ☐ Detailní
☐	Penetrační test serverových technologií	☐ Základní ☐ Detailní
Charakter služby (viz 5.1.2)		
☐	Double blind	
☐	Blind	
☐	Black box	
☐	Gray box	
☐	White box	

Tato tabulka definuje požadované typy a oblasti penetračních testů

4.1 Typy penetračních testů

- Externí penetrační testy

Zde se jedná o prověření perimetru na základě přístupu z internetu v rozsahu prověření zabezpečení DMZ, firewallu, serverů jak v DMZ tak v LAN a web aplikací.

- Interní penetrační testy

Zde se jedná o řízenou simulaci útoku z vnitřní sítě na servery a aplikace.

- Sociální penetrační testy

Zde se jedná o prověření dodržování procesů, postupů a bezpečnostních zásad v rámci organizace.

Zvolené typy jsou označeny v Tabulce 1.

4.2 Oblasti penetračních testů

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

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

Zvolené části jsou označeny v Tabulce 1.

4.3 Charakter realizace služby

Služba je realizována následujícími možnými způsoby:

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

Zvolený charakter služby je označen v Tabulce 1.

4.4 Rozsah služby

Služba je poskytována, pro oblast penetračních testů (viz 5.1.2), ve dvou variantách:

- Základní penetrační test
- Detailní penetrační test

Zvolený rozsah je označen v Tabulce 1.

4.5 Základní penetrační test:

- Test zaměřený na odhalení nejzávažnějších zranitelností.

- Přehledový test s využitím automatických testovacích nástrojů.
- Manuální testování nejzávažnějších nalezených zranitelností.

4.6 Detailní penetrační test:

- Test zaměřený na komplexní bezpečnostní audit.
- Přehledový test s využitím automatických testovacích nástrojů.
- Detailní manuální testování všech nalezených zranitelností.
- Návrh a provedení kombinovaných útočných scénářů.
- Test vhodný zejména pro rozsáhlé webové aplikace vyžadující vysoké zabezpečení.

4.7 Metodika realizace služby

Pro realizaci služby je používána uznávaná metodika Penetration Testing Execution Standard (PTSE), dle které jsou vždy realizovány, pro zvolený rozsah, následující kroky.

4.8 Vstupní analýza – Detailní naplánování bezpečnostního testu

Během této fáze jsou připravovány podklady pro samotné testování a pasivní analýza datových toků v segmentu sítě, kde bude penetrační test probíhat. v případě White-Box Testingu budou bohatým informačním zdrojem podklady od zákazníka. Vždy budou využity veřejně dostupné informace a další nástroje (manuální nebo semiautomatické) pro získání dodatečných podkladů. Na základě získaných informací jsou zmapovány cíle pro následnou fázi testování. Použité nástroje jsou vybírány tak, aby byly maximálně efektivní pro jednotlivé fáze penetračního testu. Jsou kombinovány komerční i open-source nástroje tak, aby prováděné testy vedly k odhalení problémů, ale zároveň je kladen důraz na rychlost provádění testů a tím i celkové snížení nákladů.

4.9 Testování – Řízení (koordinace) a provedení vlastního bezpečnostního testování

Během testování jsou postupně vybírány cíle, které penetrační tester podrobuje zkoumání za pomoci různých nástrojů (automatických, semiautomatických a manuálních). Pokud je nalezeno chování, které by mohlo ukazovat na přítomnost zranitelnosti, je následně provedena série testů, která má za úkol ověřit možnost jejího zneužití. Při ověřování zranitelností je kladen velký důraz na to, aby nebyla ohrožena stabilita služby nebo integrita a důvěrnost dat (např.: pokud je objevena zranitelnost, která umožňuje útočníkovi získat uživatelské jméno a heslo, bude toto demonstrováno pouze na uživatelském jméně a heslo nebude zahrnuto v žádném z výstupů testování). Během testování může dojít k objevení dodatečných cílů, které nebyly zmapovány během průzkumné fáze. Ty jsou do testování dodatečně zahrnuty. Po vyčerpání a zdokumentování všech cílů je testování ukončeno.

4.10 Výstupní dokumentace – Reportování výsledků

Report penetračního testu obsahuje zpravidla tři typy informací:

Manažerské shrnutí – podává základní přehled o průběhu testu, vyhodnocení úrovně zabezpečení testovaného objektu a obecná doporučení pro zvýšení úrovně zabezpečení. Přehledně mapuje nejrizikovější oblasti.

Technický popis nálezů – detailní popis zranitelností a potenciálně nebezpečných konfigurací kategorizovaný podle nebezpečnosti. Součástí je informace o tom, kde se zranitelnost vyskytuje, jak ji zneužít a co může útočník zneužitím zranitelnosti získat.

Navrhovaná opatření – opatření se týkají vždy konkrétního nálezu, v reportu jsou navrženy konkrétní série kroků pro odstranění dané zranitelnosti, případně snížení pravděpodobnosti jejího zneužití (např. způsob sanace vstupů webové aplikace, nutná verze softwaru nebo softwarového modulu).

5 KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

Služba je poskytována dle vzájemně odsouhlaseného časového harmonogramu včetně dodržení termínů a časů provádění stanovených testů.

6 PŘEDPOKLADY PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY

Objednatel provede nezbytná organizační opatření na základě konkrétní specifikace služby dle její vstupní analýzy a poskytne potřebné informace/dokumentaci.

Objednatel stanoví seznam oprávněných osob pro řízení této služby. Objednatel je povinen každou změnu oprávněných osob prokazatelně oznámit Poskytovateli.

7 PRINCIP STANOVENÍ CENY

Cena bude stanovena v souladu s článkem 2, odstavcem 2.4 Smlouvy a následně uvedena v konkrétní Nabídce a navazující Objednávce. To vše na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy pro následné poskytování Služby KL04.

Výsledná cena Služby KL04 se stanoví jako součin množství požadovaných rolí a jednotek a jejich jednotkové ceny uvedené v Příloze č. 2 a č.10 Smlouvy.

8 SMLUVNÍ POKUTY

V případě prodlení Poskytovatele s dodáním Předmětu plnění specifikovaném v 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.

9 POUŽITÉ VÝRAZY

Výraz	Popis
Penetrační testování	Penetrační testování je typ bezpečnostního testování, které simuluje útok na počítačový systém nebo síť s cílem identifikovat zranitelnosti a slabiny, které by mohli útočníci zneužít. Cílem penetračního testu je identifikovat slabá místa zabezpečení dříve, než je mohou zneužít zákeřní hackeři.
Systém	V souvislosti s počítačovou technologií se systémem rozumí počítačový systém, který se skládá z hardwaru, softwaru a dat. Hardwarové součásti počítačového systému zahrnují fyzické komponenty, jako je procesor, paměť a úložná zařízení, zatímco softwarové součásti zahrnují operační systém, aplikace a obslužné programy. Do datových komponent počítačového systému patří všechny informace, které jsou uloženy a zpracovávány hardwarem a softwarem.

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 1 – KL 05 Konzultace v oblasti informační a kybernetické bezpečnosti

KATALOGOVÝ LIST č. 05

Název služby	**Konzultace v oblasti informační a kybernetické bezpečnosti**

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Konzultace v oblasti informační a kybernetické bezpečnosti (dále jen **„Služba KL05"**) je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL05.

Název milníku	**Termín splnění milníku**
Zahájení poskytování Služby KL05	Na základě Objednávky
Ukončení poskytování Služby KL05	Na základě Objednávky

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba Konzultace v oblasti informační a kybernetické bezpečnosti bude poskytována v režimu dle popisu v tabulce:

Režim poskytování Služby KL05	**Doba poskytování Služby KL05**
Standardní provozní doba	V pracovní dny (5x8) 8–16 h

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 Vstupy

Vstupy dodané Objednatelem pro Službu KL05 jsou:

- Požadavky Objednatele stanovené v dané Objednávce, a to včetně požadavků na výkon činností jednotlivých rolí dle kapitoly 5 tohoto katalogového list.;

3.2 Výstupy

Výstupy Služby KL05 jsou:

- Poskytování Služby KL05;
- měsíční zpráva o stavu služby v souladu s kapitolou 5.8 tohoto katalogového listu;
- výstupy na základě požadavků Objednatele stanovených v dané Objednávce, a to včetně požadavků na výkon činností jednotlivých rolí dle kapitoly 5 tohoto katalogového listu.

4 POPIS ROZSAHU SLUŽBY

Služba Konzultace v oblasti informační a kybernetické bezpečnosti zahrnuje poskytnutí konzultací při implementaci a rozvoji informačních systémů a SŘBI Objednatele, poskytnutí konzultací a součinnosti v oblasti kybernetické bezpečnosti pro GFŘ, podpora Objednatele při ověřování a testování Služeb v oblasti informační a kybernetické bezpečnosti. Podrobná specifikace jednotlivých rolí a vykonávaných činností je popsána v kapitole 5 tohoto katalogového listu.

5 POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL05

Popis pracovní náplně jednotlivých rolí odpovídá obvyklé odborné náplni a odpovědnosti příslušné role.

5.1 Analytik kybernetické bezpečnosti

Analytik kybernetické bezpečnosti je osoba, která:

- 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.

5.2 Architekt kybernetické bezpečnosti

Architekt kybernetické bezpečnosti je osoba, která:

- zajišťuje povinnosti bezpečnostní role vycházející ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně 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.

5.3 Manažer rozvoje služeb kybernetické bezpečnosti

Manažer služeb kybernetické bezpečnosti je osoba, která:

- poskytuje konzultace v oblasti systému řízení bezpečnosti informací/kybernetické bezpečnosti;
- připravuje a prezentuje návrhy možného rozvoje činností v oblasti kybernetické bezpečnosti;
- vede rozvojové projekty ve všech fázích – inicializace, plánování, realizace, monitoring a reporting, prezentace výstupů, vyhodnocení a uzavření; zpracovává časový a finanční plán realizace projektu; má odpovědnost za realizaci projektu v souladu se schváleným časovým harmonogramem a rozpočtem; vede projektovou dokumentaci;
- řídí procesy zřízení služeb včetně sledování a reportování dodržování časového harmonogramu, odpovídá za zřízení služby ve sjednaném termínu a kvalitě;
- účastní se jednání s pracovníky Objednatele;
- zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem;
- koordinuje a řídí implementaci projektových řešení vč. vedení dokumentace v oblasti kybernetické bezpečnosti.

5.4 Manažer kybernetické bezpečnosti

Manažer kybernetické bezpečnosti je osoba, která:

- zajišťuje povinnosti bezpečnostní role vycházející ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti);
- poskytuje odborné konzultace v oblasti systému řízení bezpečnosti informací/kybernetické bezpečnosti;
- zajišťuje prosazování bezpečnosti informací v rámci organizace objednatele;
- metodicky řídí procesy systému řízení bezpečnosti;
- zajišťuje tvorbu, aktualizaci a realizaci kybernetické bezpečnostní politiky a další dokumenty organizace;
- koordinuje tvorbu bezpečnostního konceptu organizace, konceptu plánu obnovy, havarijních plánů a ostatních dílčích konceptů a systémových bezpečnostních pravidel, jakož i vydávání doplňujících pravidel a vodítek celkové kybernetické bezpečnosti;
- provádí iniciaci, sledování a vyhodnocování implementace opatření kybernetické bezpečnosti;
- ověřuje a vede vyšetřování kybernetických bezpečnostních událostí a incidentů;
- určuje způsoby realizace stanovených bezpečnostních politik;
- zpracovává bezpečnostní dokumentaci a procesy;
- monitoruje výkonnosti systému řízení bezpečnosti informací a účinnosti bezpečnostních opatření;
- zajišťuje zvyšování povědomí zaměstnanců organizace o kybernetické bezpečnosti;
- připravuje podklady pro přezkoumání systému řízení bezpečnosti informací vedením organizace;
- účastní se jednání s pracovníky Objednatele;

- zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem;
- provádí analýzu, sběr, dekompozici a syntézu získaných informací a navrhuje implementaci bezpečnostního monitoringu.

5.5 Bezpečnostní administrátor ICT

Bezpečnostní administrátor ICT je osoba, která:

- spolupracuje s administrátory ICT a bezpečnostními správci IS při připojování zdrojových logů do SIEM;
- kontroluje konfiguraci bezpečnostních prvků nasazených v ICT;
- provádí kontroly aktiv objednatele;
- spolupracuje při tvorbě bezpečnostní dokumentace ICT;
- podílí se na definici use-case pro jednotlivé ICT;
- účastní se jednání s pracovníky Objednatele;
- zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem;
- spolupracuje na analýze, sběru, dekompozici a syntéze získaných informací a navrhuje implementaci bezpečnostního monitoringu.

5.6 Organizátor vzdělávacích aktivit KB

Organizátor vzdělávacích aktivit KB je osoba, která:

- poskytuje konzultace k tvorbě návrhu ročního plánu budování bezpečnostního povědomí;
- poskytuje konzultace k tvorbě návrhů individuálních plánů vzdělávání v dané oblasti pro zaměstnance zastávající bezpečnostní role včetně certifikací;
- účastní se jednání s pracovníky Objednatele;
- zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem;
- poskytuje konzultace k vedení evidence záznamů o vzdělávání a přípravě návrhu roční zprávy o budování bezpečnostního povědomí.

5.7 Manažer řízení rizik

Manažer řízení rizik je osoba, která:

- identifikuje a hodnotí aktiva a rizika kybernetické bezpečnosti;
- posuzuje jednotlivé hrozby, dopady a zranitelnosti působící na bezpečnost organizace;
- vytváří dokumentaci k provedené analýze rizik;
- připravuje a předkládá návrhy k mitigaci rizik dle pokynů Objednatele;
- účastní se jednání s pracovníky Objednatele;
- zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem;
- vykonává metodickou a konzultační činnost v oblasti analýzy a správy rizik.

5.8 Pravidelná zpráva o stavu služby dle tohoto katalogového listu

Zpráva vyhodnocení Služby KL05, konzultace při implementaci a rozvoji informačních systémů a SŘBI Objednatele, poskytnutí součinnosti, poskytnutí činností při nastavení služeb v oblasti informační a kybernetické bezpečnosti Objednatele a jejich podpora formou poskytnutí činností rolí – obsahuje tyto informace:

- Období poskytování Služby KL05;
- Režim poskytování Služby KL05;

- Popis rozsahu Služby KL05;
- Výčet realizovaných činností za dané období;
- Přehled poskytování Služby KL05. (přehled požadovaných a realizovaných činností jednotlivých rolí včetně jejich čerpání v Člověkoden v rámci daného období).

6 SOUČINNOST PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY

Objednatel stanoví seznam určených osob pro plnění Služby KL05, 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 Služby KL05 při nominacích kompetentních osob poskytujících součinnost při zpracování výstupů Služby KL05 na straně Objednatele a jeho smluvních partnerů. Zejména se jedná o nominace příslušných rolí Poskytovatele do realizačních týmů a stanovení jejich potřebných odpovědností a kompetencí s ohledem na poskytovanou Službu;

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 KL05.

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

Požadavky na poskytnutí jednotlivých rolí jsou po uzavření odpovídající objednávky podávány do aplikace Service Desk Poskytovatele.

7 PRINCIP STANOVENÍ CENY

Cena bude pro následné poskytování Služby KL05 stanovena v souladu s článkem 2, odstavcem 2.4 Smlouvy a následně uvedena v konkrétní Nabídce a navazující Objednávce. To vše na základě požadavku Objednatele.

Výsledná cena Služby KL05 se stanoví jako součin množství požadovaných rolí a jejich jednotkové ceny uvedené v Příloze č.2 Smlouvy.

8 POUŽITÉ VÝRAZY

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

Výraz	Popis
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.

KATALOGOVÝ LIST č. 06

Název služby	Vulnerability management

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Vulnerability management (dále jen **„Služba KL06"**) je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL06.

Název milníku	Termín splnění milníku
Zahájení poskytování Služby KL06	Na základě Objednávky
Ukončení poskytování Služby KL06	Na základě Objednávky

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba KL06 bude poskytována v režimu, dle popisu v tabulce:

Režim poskytování Služby KL06	Doba poskytování Služby KL06
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 KL06 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

Výstupy Služby KL06 jsou:

- Poskytování Služby KL06;

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

4 POPIS ROZSAHU SLUŽBY

Služba KL06 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 KL06 je skenování zranitelností probíhající jedenkrát měsíčně nebo manuálním Ad-hoc skenem (např. při zveřejnění kritické zranitelnosti). Služba KL06 je realizována v rozsahu definovaných aktiv Objednatelem.

Služba KL06 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 KL06. 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 KL06 probíhá dle metodiky NIST.

Služba KL06 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 KL06 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 KL06 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 KL06, poskytováno vždy)	
☒	Příprava a průběžná úprava skenovacích scénářů
☒	Počáteční inicializační sken
☒	Periodický sken
☒	Ad-hoc sken
☒	Zpracování zprávy o stavu Služby KL06 dle tohoto katalogového listu určené Objednateli (předávána v měsíčním intervalu)
Část 2 – Ostatní součásti služby Vulnerability management povinné k naplnění vybraných opatření (nedílné součásti KL06, poskytováno vždy)	

☒	Vulnerability management – Konzole
☒	Vulnerability management – Engine
Část 3 - Doplňkové služby – Vulnerability management	
☐	Virtualizační prostředí pro provozování Služby KL06 v prostředí SPCSS

4.1 Plnění legislativních povinností Objednatele

Služba KL06 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. KL06 obsahuje obecný výčet požadavků VoKB, pro jejichž naplnění Objednateli služba KL06 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 KL06 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 KL06 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 KL06), 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 KL06 nezahrnuje organizační a technická opatření SŘBI Objednatele. Součástí Služby KL06 není tvorba politik, vyjma dokumentace dle kapitoly 3 tohoto katalogového listu. Služba KL06 nepokrývá výše zmíněné ustanovení VoKB v plném rozsahu, ale výstupy Služby KL06 jsou využívány při realizaci jednotlivých organizačních a technických opatření v rámci SŘBI Objednatele.

5 POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL06

Předmětem Služby KL06 je skenování zranitelností probíhající jedenkrát měsíčně nebo manuálním Ad-hoc skenem. Služba KL06 se skládá z:

- Komponenty služby KL06

- Fáze služby KL06

5.1 Komponenty Služby KL06

Jednotlivé komponenty Služby KL06:

- 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 KL06

Jednotlivé kroky poskytování Služby KL06:

- 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.

- 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 KL06;
- Režim poskytování Služby KL06;
- Popis rozsahu Služby KL06;
- Seznam aktiv skenovaných službou KL06 včetně jejich detailního popisu;
- Přehled výskytu zranitelností zjištěných službou KL06;
- Přehled závažných zranitelností podle operačních systémů zjištěných službou KL06;
- Výpis závažných zranitelností (úroveň zranitelnosti 8-10) zjištěných službou KL06;
- Výpis zranitelností nižší úrovně zjištěných službou KL06;
- Přehled Ad-hoc skenů provedených v rámci služby KL06;
- Doporučení, jak zjištěné zranitelnosti řešit.

5.4 Cílová prostředí

Službu KL06 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 KL06 bude stanovena na základě analýzy dle kapitoly 3.1.

6 SLA PARAMETRY

Poskytovatel je povinen poskytovat Službu KL06 dle Smlouvy v rozsahu definovaném objednávkou, a to v níže uvedených parametrech.

Ovlivnění chodu všech částí Služby KL06 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 KL06.

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 KL06 – Příprava a průběžná úprava skenovacích scénářů, Počáteční inicializační sken, Kontrolní sken, Zpracování zprávy o stavu Služby KL06 dle tohoto katalogového listu určené Objednateli (předávána v měsíčním intervalu) - neovlivňuje dostupnost a kvalitu poskytované Služby KL06 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:**

Název Služby:	Vulnerability management	
SLA parametry		
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 KL06

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 KL06 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 KL06 soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL06 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 KL06 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 KL06. Ovlivnění chodu Služby KL06 ze strany Objednatele se nezapočítává do nedostupnosti Služby KL06.

7 DOPLŇKOVÉ SLUŽBY

7.1 Virtualizační prostředí pro provozování služby v prostředí SPCSS

Doplňková služba slouží k zajištění a provozování virtualizovaného prostředí Služby KL06 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:

7.1.1 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.

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.

- **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.

- **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 Objednatele 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

Tato část specifikuje nezbytnou součinnost ze strany Objednatele:

- Objednatel stanoví Poskytovateli kontaktní osoby včetně komunikační matice pro řádné poskytování Služby KL06.
- V případě, že Objednatel využívá třetí strany pro správu, servis, podporu, konfiguraci apod. systému/ů skenovaného/ných v rámci Služby KL06, bude pro řádné poskytování Služby KL06 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.

9 PRINCIP STANOVENÍ CENY

Cena bude stanovena v souladu s článkem 2, odstavcem 2.4 Smlouvy a následně uvedena v konkrétní Nabídce a navazující Objednávce. To vše na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy pro následné poskytování Služby KL06.

V rámci Vstupní analýzy bude stanoveno množství jednotek pro zajištění řádného poskytování Služby KL06. Výsledná cena Služby KL06 se stanoví jako součin množství požadovaných rolí a jednotek a jejich jednotkové ceny uvedené v Příloze č.2 a v Příloze č.10 Smlouvy.

Vstupní analýza bude zpracovaná Dodavatelem a předaná Objednateli v rámci poskytování odpovídajícího plnění.

Realizace Vstupní analýzy je povinným vstupem pro řádné stanovení ceny Služby KL06, kdy je rozhodné naplnění zpracování dílčího plnění dle výše zmíněné Rámcové smlouvy, a to:

- zpracování dokumentu „Závěrečná zpráva řešení Vulnerability managementu v rozsahu definovaném Objednatelem".

Realizace ověření provozu bude zpracovaná Dodavatelem a předaná Objednateli v rámci poskytování odpovídajícího plnění.

Vstupem a povinnou podmínkou pro Realizaci ověření provozu je dokument „Závěrečná zpráva řešení Vulnerability managementu v rozsahu definovaném Objednatelem" zpracovaný dle Vstupní analýzy, dle kapitoly 3.1.

Realizace ověření provozu je povinným vstupem pro řádné stanovení ceny Služby KL06.

Služba Vstupní analýza a Realizace ověření provozu není samostatným Výstupem plnění Služby KL06 dle kapitoly 3.2. Tyto služby mohou být realizovány na základě samostatné objednávky dílčích částí Služby KL06 a KL05 (Konzultace).

10 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 110 % 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 110 % z poměrné části příslušné měsíční Ceny za Službu bez DPH za dobu přesahující hodnotu parametru doby vyřešení kritické závady dané Služby.

11 POUŽITÉ VÝRAZY

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

KATALOGOVÝ LIST č. 07

Název služby	Kompetenční centrum kybernetické bezpečnosti

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Kompetenční centrum kybernetické bezpečnosti (dále také **„Služba KL07"**) je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL07.

Název milníku	Termín splnění milníku
Zahájení poskytování Služby KL07	Na základě Objednávky
Ukončení poskytování Služby KL07	Na základě Objednávky

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba KL07 bude poskytována v režimu dle popisu v tabulce:

Režim poskytování Služby KL07	Doba poskytování Služby KL07
Standardní provozní doba	V pracovní dny (5x8) 8–16 h

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 Vstupy

Vstupy dodané Objednatelem pro Službu KL07 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.

3.2 Výstupy

Výstupy Služby KL07 jsou:

- Poskytování Služby KL07;

- 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 KL07 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 KL07, 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 KL07 – Část 1 a Část 2

Služba KL07 je služba postavená na týmu odborníků pokrývajícím všechny potřebné kompetence a znalosti se zajištěnou zastupitelností.

Služba KL07 je určena jako odborná administrativní podpora v oblasti informační a kybernetické bezpečnosti pro Objednatele. Služba KL07 zajišťuje podporu vedení a správy systému řízení bezpečnosti informací (dále také „**SŘBI**"). Služba KL07 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 KL07

Služba KL07 zahrnuje:

- administraci dokumentace Objednatele v Nástroji pro podporu řízení SŘBI;
- metodickou podporu Objednatele;
- 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 KL07 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 KL07, 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.

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 KL07 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 KL07 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 KL07. 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 KL07.

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 KL07. 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 KL07 je metodická podpora Objednatele v oblasti informační a kybernetické bezpečnosti. Podporu poskytují odborníci SPCSS.

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 KL07;
- Režim poskytování Služby KL07;
- Popis rozsahu Služby KL07;
- Provozovaná prostředí;
- Aktivity Služby KL07;
- Řízení provozu Služby KL07;
- Návrh na nápravná opatření a doporučení.

6 SLA PARAMETRY

Poskytovatel je povinen poskytovat Službu KL07 dle Smlouvy v rozsahu definovaném objednávkou, a to v níže uvedených parametrech.

Ovlivnění chodu všech částí Služby KL07 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 KL07.

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 KL07 – 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 KL07 – Část 1 a Část 2 ve výše definovaném rozsahu do okamžiku obnovení poskytování. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti Služby KL07 – 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 KL07 – Zpracování zprávy o stavu Služby KL07 dle tohoto katalogového listu určené Objednateli (předávána v měsíčním intervalu) - neovlivňuje dostupnost a kvalitu poskytované Služby KL07 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:

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

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 KL07.

6.1.2 Požadované lhůty pro obnovení Služby KL07 – 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 KL07 – Části 1 a Část 2

Kategorizace provozních incidentů:	
Incident kategorie A	Služba KL07 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 KL07, 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

6.2 REAKČNÍ DOBY A DOBY PODPORY SLUŽBY KL07

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 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 KL07 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 KL07 soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL07 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 KL07 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 KL07. Ovlivnění chodu Služby KL07 ze strany Objednatele se nezapočítává do nedostupnosti Služby KL07.

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 KL07 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 KL07 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;
- 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 KL07, 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 KL07 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 KL07;

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 KL07.

Hlášení poruchy Služby KL07 oznamuje Objednatel na Service Desk Poskytovatele.

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

9 PRINCIP STANOVENÍ CENY

9.1 Administrace v Nástroji pro podporu řízení SŘBI

Cena bude stanovena v souladu s článkem 2, odstavcem 2.4 Smlouvy a následně uvedena v konkrétní Nabídce a navazující Objednávce. To vše na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy pro následné poskytování Služby KL07.

V rámci Vstupní analýzy bude stanoveno množství jednotek pro zajištění řádného poskytování Služby KL07. Výsledná cena Služby KL07 se stanoví jako součin množství požadovaných jednotek a rolí a jejich jednotkové ceny uvedené v **Příloze č.2** a v **Příloze č.10** Smlouvy.

Vstupní analýza bude zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování plnění analytické činnosti související s analýzou a přípravou Služeb v oblasti informační a kybernetické bezpečnosti systémů Objednatele, zpracování návrhu rozsahu testování služby pro vybraný systém a jeho oblast, tj. dle smlouvy uzavřené mezi Poskytovatelem a Objednatelem.

Realizace Vstupní analýzy je povinným vstupem pro řádné stanovení ceny Služby KL07, kdy je rozhodné naplnění zpracování dílčího plnění dle smlouvy, a to:

zpracování dokumentu „Návrh řešení správy a řízení dokumentace v rozsahu vybraného SŘBI".

Realizace ověření provozu bude zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování plnění poskytnutí podpory testování služby a zpracování vyhodnocení ověření služby formou jednorázových nebo měsíčně se opakujících činností, tj. dle smlouvy uzavřené mezi Poskytovatelem a Objednatelem.

Vstupem a povinnou podmínkou pro Realizaci ověření provozu je dokument **„**Návrh řešení správy a řízení dokumentace v rozsahu vybraného SŘBI**"** zpracovaný Poskytovatelem dle Vstupní analýzy.

Realizace ověření provozu je povinným vstupem pro řádné stanovení ceny Služby KL07, kdy je rozhodné naplnění zpracování dílčího plnění dle smlouvy, a to:

- zpracování dokumentu „Vyhodnocení Služby Poskytnutí podpory testování služby a zpracování vyhodnocení ověření služby formou jednorázových nebo měsíčně se opakujících činností v rozsahu vybraného SŘBI".

Služba Vstupní analýza a Realizace ověření provozu není samostatným Výstupem plnění Služby KL07 dle kapitoly 3.2. Tyto služby mohou být realizovány na základě samostatné objednávky dílčích částí Služby KL07 a KL05 (Konzultace v oblasti informační a kybernetické bezpečnosti).

9.2 Metodická podpora

Cena bude stanovena na následujícím principu a dle následujících pravidel:

Cena za jeden člověkoden (jeden člověkoden se skládá z osmi člověkohodin) pro danou roli dle Smlouvy * počet prokazatelně vynaložených člověkodnů na poskytování Metodické podpory v rámci dané role definované dle Smlouvy v předmětném kalendářním měsíci na základě dané Objednávky.

Přičemž ceny za jeden Poskytovatelem vynaložený člověkoden pro jednotlivé role definované dle Smlouvy jsou uvedeny ve Smlouvě. Poskytovatel bere na vědomí a souhlasí s tím, že jednotlivé doby poskytnuté na Metodickou podporu v rámci příslušného kalendářního měsíce se sčítají dle vykázaného a Objednatelem schváleného času stráveného na poskytování Metodické podpory, přičemž Poskytovatelem může být účtován čas s přesností na 1/8 člověkodne.

Poskytnutí jednotlivých rolí je realizováno zejména pracovníky SPCSS a jednotlivé činnosti jsou realizovány prostřednictvím odpovídajících rolí dle Smlouvy.

9.3 Zvyšování bezpečnostního povědomí

Cena bude stanovena v souladu se Smlouvou a na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy stávajícího a očekávaného stavu Objednatele k doplňkové službě Zvyšování bezpečnostního povědomí.

Vstupní analýza stavu bude použita pro návrh struktury a harmonogramu vzdělávání v oblasti Zvyšování bezpečnostního povědomí a zajištění souladu s legislativními požadavky a interními předpisy.

Výsledná cena doplňkové služby – Zvyšování bezpečnostního povědomí se stanoví na základě Vstupní analýzy jako kombinace požadovaných jednotek, jejich množství a jednotkové ceny uvedené ve Smlouvě.

Vstupní analýza bude zpracovaná Poskytovatelem a předaná Objednateli jako výstup na základě samostatné objednávky dílčích částí Služby KL07 a KL05 (Konzultace v oblasti informační a kybernetické bezpečnosti). Služba Vstupní analýza a Realizace ověření provozu není samostatným Výstupem plnění Služby KL07 dle kapitoly 3.2.

Realizace Vstupní analýzy je povinným vstupem pro řádné stanovení ceny doplňkové služby – Zvyšování bezpečnostního povědomí, kdy je rozhodné naplnění zpracování dílčího plnění dle výše zmíněné Rámcové smlouvy, a to:

- zpracování dokumentu „Vstupní analýzy v oblasti zvyšování bezpečnostního povědomí".

10 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 110 % 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 110 % 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.

11 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.

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 1 – KL 08 Správa privilegovaných účtů

KATALOGOVÝ LIST č. 8

Název služby	**Správa privilegovaných účtů**

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Správa privilegovaných účtů (dále jen **„Služba KL08"**) je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL08.

Název milníku	**Termín splnění milníku**
Zahájení poskytování Služby KL08	Na základě Objednávky
Ukončení poskytování Služby KL08	Na základě Objednávky

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba KL08 bude poskytována v režimu, dle popisu v tabulce:

Režim poskytování Služby KL08	**Doba poskytování Služby KL08**
Standardní provozní doba – Část 1 a 2	Nepřetržitě (24x7)
Poskytování podpory Služby KL08	V pracovní dny (5x8) 8–16 h

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 Vstupy

Vstupy dodané Objednatelem pro Službu KL08 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 KL08 jsou:

- Poskytování Služby KL08;
- 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 KL08 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 KL08 (nedílné součásti KL08, 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 KL08 nezahrnuje organizační opatření SŘBI Objednatele. Součástí Služby KL08 dle tohoto katalogového listu není tvorba politik.

5 POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL08

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 KL08

Jedná se o poskytování podpory související s poskytováním Služby KL08. 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 KL08;
- Režim poskytování Služby KL08;
- Popis rozsahu Služby KL08;
- Provozovaná prostředí;
- Aktivity Služby KL08;
- Řízení provozu Služby KL08;
- Návrh na nápravná opatření a doporučení.

7 SLA PARAMETRY

Poskytovatel je povinen poskytovat službu KL08 dle Smlouvy v rozsahu definované objednávkou, a to v níže uvedených parametrech.

Ovlivnění chodu všech částí Služby KL08 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 KL08.

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:**
Část 1 – Řízení přístupu privilegovaných účtů, Session Recording	99,5 %	každý čtvrtek, vždy 19:00-24:00

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

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

Nedostupnost Služby KL08 – 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 KL08 – Část 1 a Část 2 ve výše definovaném rozsahu do okamžiku obnovení poskytování. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti Služby KL01 – 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 KL08.

7.1.2 Požadované lhůty pro obnovení Služby KL08 – 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 KL08 – 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 KL08

Podpora dle Služby KL08 je určena k zajištění rozvoje a podpory jejího efektivního využívání. Doba reakce na požadovanou podporu Služby KL08 je počítána od zadání požadavku do aplikace Service Desk Poskytovatele. Za reakci je považována odpověď na požadavek s návrhem dalšího postupu řešení.

Podpora Služby KL08 je poskytována v režimu 8x5.

Název Služby:	**Správa privilegovaných účtů**	
SLA parametry		
Podpora Služby KL08 – 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 KL08

7.3 Plánované odstávky

V rámci poskytování Služby KL08 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 KL08 soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL08 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 KL08 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 KL08. Ovlivnění chodu Služby KL08 ze strany Objednatele se nezapočítává do nedostupnosti Služby KL08.

8 SOUČINNOST PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY KL08

- 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.

9 PRINCIP STANOVENÍ CENY

Cena bude stanovena v souladu s článkem 2, odstavcem 2.4 Smlouvy a následně uvedena v konkrétní Nabídce a navazující Objednávce. To vše na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy pro následné poskytování Služby KL08.

V rámci Vstupní analýzy bude stanoveno množství jednotek pro zajištění řádného poskytování Služby KL08. Výsledná cena Služby KL08 se stanoví jako součin množství požadovaných jednotek a rolí a jejich jednotkové ceny uvedené v Příloze č.2 a v Příloze č.10 Smlouvy.

Vstupní analýza bude zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování plnění analytické činnosti související s analýzou a přípravou Služeb v oblasti informační a kybernetické bezpečnosti systémů Objednatele, zpracování návrhu rozsahu testování služby pro vybraný systém a jeho oblast dle smlouvy uzavřené mezi Poskytovatelem a Objednatelem.

Realizace Vstupní analýzy je povinným vstupem pro řádné stanovení ceny Služby KL08, kdy je rozhodné naplnění zpracování dílčího plnění dle výše zmíněné Rámcové smlouvy, a to:

- zpracování dokumentu „Návrh řešení správy privilegovaných účtů ICT systémů v rozsahu vybraného ICT".

Realizace ověření provozu bude zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování plnění poskytnutí podpory testování služby a zpracování vyhodnocení ověření služby formou jednorázových nebo měsíčně se opakujících činností dle smlouvy uzavřené mezi Poskytovatelem a Objednatelem.

Vstupem a povinnou podmínkou pro Realizaci ověření provozu je dokument „Návrh řešení správy privilegovaných účtů ICT systémů GFŘ v rozsahu vybraného ICT" zpracovaný dle Vstupní analýzy.

Realizace ověření provozu je povinným vstupem pro řádné stanovení ceny Služby KL08, kdy je rozhodné naplnění zpracování dílčího plnění dle výše zmíněné Rámcové smlouvy, a to:

- zpracování dokumentu „Vyhodnocení Služby Poskytnutí podpory testování služby a zpracování vyhodnocení ověření služby formou jednorázových nebo měsíčně se opakujících činností v rozsahu vybraného ICT".

Služba Vstupní analýza a Realizace ověření provozu není samostatným Výstupem plnění Služby KL01 dle kapitoly 3.2. Tyto služby mohou být realizovány na základě samostatné objednávky dílčích částí Služby KL01 a KL05 (Konzultace).

10 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 110 % 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 110 % z poměrné části příslušné měsíční Ceny za Službu bez DPH za dobu přesahující hodnotu parametru doby vyřešení kritické závady dané Služby.

11 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.

KATALOGOVÝ LIST Č. 09
Služby IaaS – Landing zóna pro provoz IS Objednatele

Obsahem katalogového listu je služba IaaS – Landing zóna (dále jako „Služba"), jejíž předmětem poskytnutí síťové infrastruktury SPCSS (dále jako „Poskytovatel") a konektivity z prostředí Poskytovatele pro účely provozu informačních systémů Ministerstvo zahraničních věcí (dále jako „Objednatel") umístěných do prostředí Poskytovatele.

Čerpané infrastrukturní zdroje jsou uvedeny v oboustranně odsouhlasené dokumentaci: High-level design.

1 SLUŽBA POSKYTOVATELE PRO INFORMAČNÍ SYSTÉMY OBJEDNATELE

1.1 Období poskytování Služby

Služba je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby.

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

1.2 Režim poskytování Služby

Služba dle čl. 1 tohoto katalogového listu bude poskytována v režimu:

Režim poskytování Služby	Doba poskytování
Provozní doba Služby	24x7
Provozní doba podpory Service Desk	24x7

1.3 Popis rozsahu Služby

Předmětem Služby je poskytnutí následujících infrastrukturních komponent:

- Poskytování bezpečného komunikačního rozhraní s parametry:
  - Konektivita a FW propustnost prostředí do sítě internet v lokalitách Vápenka a Zeleneč o rychlosti <100> Mbit/s
  - Konektivita a FW propustnost prostředí do CMS2 v lokalitách Vápenka a Zeleneč o rychlosti <100> Mbit/s
  - Konektivita mezi prostředím Objednatele a prostředím Poskytovatele z lokalit Vápenka a Zeleneč prostřednictvím 2 linek DWDM lambda 10GE
  - Konektivita do prostředí veřejného cloudu Azure prostřednictvím VPN S2S z prostředí Vápenka a Zeleneč o rychlosti <100> Mbit/s
  - Ochrana vystaveného rozhraní aplikace do sítě internet DDoS protektorem
  - Bezpečnostní perimetr firewall
  - Služby aplikačního load balancing provozu a vIP pro přístup do CMS2

- Řízení provozu Služby:
  - Provozní monitoring síťové infrastruktury
  - Instalace a konfigurace síťových zařízení
  - Upgrade a opravy síťových prvků
  - Údržba síťové infrastruktury dle požadovaných výkonnostních parametrů
  - Řešení problémů a incidentů identifikovaných v síťové infrastruktuře dle ISO standardů (ČSN ISO/IEC 20000-1:2019, ČSN EN ISO 9001:2016)
  - Vyhodnocování a optimalizace výkonu sítě a síťových prvků
  - Údržba dokumentace o konfiguraci síťové infrastruktury a jejích prvcích
  - Testování změn provedených v síťové infrastruktuře
  - Uchování provozních logů

- Řízení provozu a dohled nad kvalitou poskytované Služby:
  - Projektové a organizační řízení služby na straně Poskytovatele během přípravy a následného provozu Služby

- Bezpečnost:
  - Zajištění trvalého bezpečnostního monitoringu infrastrukturních komponent Služby, a to dle ZoKB a VoKB

- Požadované součinnosti poskytované Objednatelem:
  - Objednatel zajistí na své straně nominaci odpovědných osob za účelem projektového řízení a odpovídající technické role pro období implementace služby do prostředí Poskytovatele infrastruktury
  - Objednatel se zavazuje poskytnout nezbytné osobní údaje určené pro zajištění VPN přístupu určeným pracovníkům Objednatele do prostředí Poskytovatele.

- Objednatel se zavazuje poskytnout nezbytné údaje a součinnost při realizaci veškerých konektivit, které jsou součástí Služby
- Objednatel se zavazuje poskytnout součinnost při čerpání služeb CMS2

V termínu zahájení poskytování Služby podle tohoto katalogového listu má Objednatel vybudované prostředí pro provoz informačních systémů dle dokumentu High-level design.

Součástí Služby není poskytnutí jakýchkoliv dalších licencí, podlicencí ani sekundárních podlicencí pro Objednatele.

1.4 Zajištění servisní podpory Služby

Komunikačním kanálem pro hlášení incidentů a požadavků určenými pracovníky Objednatele je Service Desk Poskytovatele (dále jako „Service Desk"). Service Desk je dostupný v režimu 24x7.

ServiceDesk je pracoviště Poskytovatele přijímající servisní hlášení od určených osob Objednatele zadáním požadavku v aplikaci, telefonicky nebo e-mailem. V případě vzniku incidentu, vzniku požadavku na konfigurační úpravu Služby nepřesahující parametrický rámec tohoto katalogového listu a na konzultace ke Službě, jsou k dispozici následující kontakty Poskytovatele:

- aplikace: https://servicedesk.spcss.cz/
- telefon: [redacted]
- e-mail: [redacted]

Plnění smluvních SLA parametrů Služby souvisejících s řešením incidentů bude vyhodnocováno na základě údajů zaznamenaných v Service Desku.

Servisní podpora bude primárně zajišťovaná prostřednictvím pracovníků Poskytovatele nebo jeho dodavatelů na základě smluv uzavřených mezi Poskytovatelem a jeho servisními dodavateli.

1.5 Kvalitativní parametry Služby

1.5.1 Odstraňování závad (incident)

Závada je neplánované přerušení nebo zhoršení kvality Služby. Z pohledu závažnosti se závady dělí na následující kategorie:

- Kritická – závada, při níž není Služba použitelná ve svých základních funkcích nebo je zcela nefunkční;
- Závažná – závada, kdy je Služba ve svých funkcích degradovaná natolik, že tento stav omezuje její běžné používání;
- Nezávažná – drobná závada, která nijak významně neovlivňuje Službu.

Požadované lhůty pro Odstranění závady jsou uvedeny v následující tabulce

Lhůta pro Odstranění závady			
Kategorie závady	**Kritická (A)**	**Závažná (B)**	**Nezávažná (C)**
Popis SLA	7 dnů v týdnu, 24 hodin denně v době od 0:00 do 24:00 hodin, s povinností oznámit zahájení řešení do 30 minut od nahlášení a odstranit závadu do 4	7 dnů v týdnu, 13 hodin denně v době od 7:00 do 20:00 hodin, s povinností oznámit zahájení řešení do 1 hodiny od nahlášení a	5 pracovních dnů v týdnu, 11 hodin denně v době od 7:00 do 18:00 hodin, s povinností oznámit zahájení řešení nejpozději následující pracovní den

Lhůta pro Odstranění závady			
Kategorie závady	**Kritická (A)**	**Závažná (B)**	**Nezávažná (C)**
	hodin od nahlášení Servisního hlášení.	odstranit závadu do 8 hodin od nahlášení Servisního hlášení.	a odstranit závadu do 55 hodin od nahlášení Servisního hlášení.
Provozní doba (dny)	7 dnů v týdnu	7 dnů v týdnu	5 pracovních dnů v týdnu
Provozní doba (hodiny)	Nepřetržitě	7:00 – 20:00	7:00 – 18:00
Výjimky z provozní doby	nejsou	nejsou	nejsou
Garantovaný čas reakce operátora	15 minut	30 minut	30 minut
Garantovaný čas zahájení prací na odstranění závady	+ 30 minut	+1 hodina	následující pracovní den
Garantovaný čas odstranění závady	+ 4 hodiny	+8 hodin	+55 hodin

1.5.2 Řešení provozních požadavků (požadavek)

Požadované lhůty pro Řešení provozních požadavků jsou uvedeny v následující tabulce

Lhůta pro Řešení provozních požadavků	
Popis SLA	5 pracovních dnů v týdnu, 8 hodin denně v době od 8:00 do 16:00 hodin
Provozní doba (dny)	5 pracovních dnů v týdnu
Provozní doba (hodiny)	8:00 – 16:00
Výjimky z provozní doby	nejsou
Garantovaný čas zahájení řešení požadavku	2 hodiny
Garantovaný čas vyřešení požadavku	N/A*)

*) Termín vyřešení se odvíjí od výsledku analýzy požadavku

1.5.3 Roční dostupnost Služby

Požadavek na roční dostupnost Služby podle tohoto katalogového listu je 99,99 % v každém kalendářním roce. Požadovaná roční dostupnost ve výše uvedených provozních dobách se posuzuje vždy pro aktuální kalendářní rok. Na počátku každého kalendářního roku Poskytovatel vypočítá maximální možné trvání nedostupnosti Služby pro dané období podle uvedených procentuálních hodnot požadované roční dostupnosti. Provozní požadavky nejsou součástí výše uvedené roční dostupnosti.

1.5.4 Plánované odstávky

V rámci poskytování Služby si Poskytovatel vyhrazuje právo na plánované odstávky celého nebo částí systému. Nedostupnost Služby v době plánovaných odstávek se nezapočítává do celkové roční nedostupnosti Služby.

Doba odstávky, která byla předem řádně ohlášena se nezapočítává do nedostupnosti Služby. Za ohlášení se považuje informování Objednatele e-mailem na adresu Oprávněné osoby Objednatele a to minimálně 48 hodin před zahájením odstávky. Objednatel následně vyslovuje souhlas s navrženou odstávkou, a to do 24 hodin před termínem odstávky. Ovlivnění chodu Služby ze strany Objednatele se nezapočítává do nedostupnosti Služby. V případě urgentní odstávky může být ohlášení jednostranné.

1.5.5 Definice měření dostupnosti

Dostupnost Služby je definovaná při splnění následující podmínky:

- přenosová trasa je funkční, poskytování Služby není výrazně omezeno, ztíženo nebo přerušeno

Za nahlášení nedostupnosti Služby se považuje založení odpovídajícího servisního hlášení dle postupu uvedeného v kapitole 1.4.

Dostupnost služby se vypočítá podle následujícího vzorce:

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

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 plánované odstávky.

1.5.6 Nedodržení kvalitativního parametru Služby

V případě, že ze strany Poskytovatele dojde k nedodržení kvalitativního parametru Služby a pokud se Poskytovatel s Objednatelem nedohodnou jinak, Objednateli vzniká právo na uplatnění smluvní pokuty.

Poskytovatel bude zproštěn povinnosti dodržet kvalitativní parametr Služby, pokud:

- Objednatel prokazatelně neposkytne požadovanou součinnost;
- k nedostupnosti nebo závadě dojde ze strany Objednatele mimo působnost Poskytovatele;
- k nedostupnosti došlo mimo infrastrukturu Poskytovatele;
- vyskytnou se okolnosti, které představují událost vyšší moci.

1.6 Cena za Předmět plnění

1.6.1 Příprava Služby

Poskytování Služby bude předcházet příprava, resp. součástí přípravy jsou kroky konfigurace infrastruktury dle specifikace případné zajištění přístupu určeným pracovníkům Objednatele k infrastrukturním zdrojům a nezbytná součinnost Poskytovatele Objednateli při spuštění Služby. Cena za přípravu Služby a způsob její fakturace bude uvedena do konkrétní Nabídky a následné Objednávky na základě specifikace v dokumentu High level design.

Uvedená cena odpovídá rozsahu specifikovanému v odstavci 1.3 této přílohy:

Příprava	Cena v Kč bez DPH	DPH	Cena v Kč včetně DPH
Celková cena za přípravu	***Výše bude stanovena dle HLD***		

1.6.2 Měsíční cena za Službu

Uvedená měsíční cena Služby odpovídá rozsahu specifikovanému v odstavci 1.3 této přílohy. Paušální měsíční cena za Službu a způsob její fakturace bude uveden do konkrétní Nabídky a následné Objednávky na základě specifikace v dokumentu High level design.

Služba	Cena v Kč bez DPH za měsíc	DPH	Cena v Kč včetně DPH za měsíc
Celková měsíční cena Služby	***Výše bude stanovena dle HLD***		

1.7 Smluvní pokuty za nesplnění parametrů poskytování Služby

Za porušení kvalitativních parametrů, nedodržení požadované lhůty pro odstranění závady ve lhůtě dle odst. 1.5.1 tohoto katalogového listu je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu za každou započatou hodinu prodlení dle následující tabulky.

Za porušení parametru nedodržení požadované roční dostupnosti Služby dle odstavce 1.5.3 tohoto katalogového listu je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu za každou 1 hodinu nedostupnosti Služby nad stanovený limit dle následující tabulky.

Název parametru	Smluvní pokuta za porušení parametru Služby v % z celkové měsíční ceny Služby bez DPH dle odst. 1.5.1 tohoto KL	Max. výše smluvní pokuty v % z celkové měsíční ceny Služby bez DPH dle odst. 1.5.1 tohoto KL	Způsob výpočtu
Dostupnost oblasti Služby	1	40	Za každou započatou hodinu nad povolený limit nedostupnosti nebo doby odstranění závady (incidentu)
Doba odstranění závady (incidentu) kategorie A	1	40	
Doba odstranění závady (incidentu) kategorie B	0,5	15	
Doba odstranění závady (incidentu) kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období, avšak je omezená do výše 50 % ceny Služeb uzavřených Objednávek dle tohoto katalogového listu.

Smluvní pokuty, jejich výše a parametry, pokud budou odlišné od tohoto katalogového listu, budou stanoveny v konkrétní Nabídce a následné Objednávce.

KATALOGOVÝ LIST Č. 10
Služby PaaS pro IS s provozní podporou 8x5

Obsahem katalogového listu je poskytnutí infrastruktury a souvisejících služeb SPCSS (dále jako „Poskytovatel") v úrovni PaaS pro IS jehož provozní doba je 8x5 (dále jen jako „Služba") pro Ministerstvo zahraničních věcí (dále jako „Objednatel").

Čerpané infrastrukturní zdroje pro Službu jsou uvedeny v oboustranně odsouhlasené dokumentaci – High-level design.

1 SLUŽBA PAAS PRO IS S PROVOZNÍ PODPOROU 8X5

1.1 Období poskytování Služby

Služba je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby.

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

1.2 Režim poskytování Služby

Služba dle čl. 1 tohoto katalogového listu bude poskytována v režimu:

Režim poskytování Služby	Doba poskytování
Provozní doba Služby	24x7
Provozní doba podpory Service Desk	8x5

*) režim poskytování Služby bude stanoven v High level designu a následně uveden v konkrétní Nabídce a navazující Objednávce

1.3 Popis rozsahu Služby

Služba bude poskytována dle rozsahu uvedeném v dokumentu High level design pro konkrétní Nabídku a navazující Objednávku. Přehled možného rozsahu služeb:

- Poskytování výpočetního výkonu a zálohovacích kapacit a dalších provozních služeb
- Poskytování správy operačních systémů (dále jako „OS") jejíž součástí jsou následující provozní činnosti:

- Instalace operačních systémů
- Instalace verzí/patchů OS v pravidelných intervalech
- Změny konfigurací OS
- Instalace kritických oprav OS
- Kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz
- Vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu)
- Profylaxe systému dle harmonogramu v měsíčních intervalech
- Instalace a konfigurace nového software
- Instalace a údržba ovladačů a firmware hardware virtualizační platformy Poskytovatele
- Správa účtů v OS
- Úpravy výkonnostních parametrů systému
- Správa souborového systému (filesystem, přístupová práva, kvóty a limity jeho použití)
- Konzultace při poskytování podpory uživatelům
- Údržba dokumentace o konfiguraci OS
- Troubleshooting OS
- Hardening OS
- Testování změn provedených v OS
- Komunikace a řešení problémů s externím suportem
- Konfigurace a nastavení firewallu v prostředí OS

- Poskytování správy databáze (dále jako „DB“) jejíž součástí jsou následující provozní činnosti:
  - Instalace databázového serveru bez poskytnutí licence
  - Administrace databáze (změny konfigurací databáze, správa účtů v databázi)
  - Instalace patchů
  - Instalace kritických oprav
  - Instalace security patchů
  - Upgrade a migrace databáze
  - Definice zálohování a obnovy dat
  - Vytvoření a správa replikací
  - Vyhodnocování výstupů z monitoringu databáze (sledování výkonnostních parametrů a zatížení databáze)
  - Úpravy výkonnostních parametrů databáze
  - Reportování výstupů z monitoringu na vyžádání
  - Preventivní údržba databázového serveru a databází
  - Restarty databází dle požadavků Objednatele
  - Odpovídání na technické dotazy Objednateli
  - Údržba dokumentace o konfiguraci databáze

- Troubleshooting databáze
- Testování změn provedených v databázi
- Komunikace a rešení problémů s externím suportem

- Poskytování bezpečného komunikačního rozhraní:
  - Zajištění komunikační infrastruktury dle KL – Landing zóna – MZV

- Řízení provozu a dohled nad kvalitou poskytované Služby:
  - Trvalý provozní dohled infrastruktury a platforem
  - Uchování provozních logů dle klasifikace systému
  - Zálohování infrastruktury a platforem do úložišť v prostředí Poskytovatele
  - Řízení provozu Služby dle dle ISO standardů (ČSN ISO/IEC 20000-1:2019, ČSN EN ISO 9001:2016)
  - Projektové a organizační řízení služby na straně Poskytovatele během přípravy a následného provozu Služby

- Bezpečnost:
  - Zajištění trvalého bezpečnostního monitoringu infrastrukturních komponent Služby, a to dle ZoKB a VoKB
- Předpoklady poskytování služeb:
  - účty s administrátorskými právy jsou v rukách Poskytovatele. Přidělení vyšších práv uživatelským nebo aplikačním účtům Objednatele je řízeno pracovníky Poskytovatele. Ve všech případech podléhá schválení ze strany Poskytovatele, toto ustanovení se vztahuje na prostředí poskytovaných Poskytovatelem formou Služby;
  - Poskytovatel instaluje vždy minimální výchozí instalaci databázového systému. S Objednatelem je pak odsouhlasen seznam úprav, které si přeje na dodávaném OS provést nad rámec minimální instalace.

- Požadované součinnosti poskytované Objednatelem:
  - Objednatel zajistí na své straně nominaci odpovědných osob za účelem projektového řízení a odpovídající technické role pro období implementace služby do prostředí Poskytovatele infrastruktury
  - Objednatel se zavazuje poskytnout nezbytné osobní údaje určené pro zajištění VPN přístupu určeným pracovníkům Objednatele do prostředí Poskytovatele.

V termínu zahájení poskytování Služby podle tohoto katalogového listu má Objednatel vybudované prostředí pro provoz IS v objemu a nastavení uvedených v dokumentu High-level design.

Součástí ceny jsou licence OS výrobce, dle požadavků specifikovaných v dokumentu High level design.

Součástí ceny nejsou licence MS SQL databází.

Součástí Služby není poskytnutí jakýchkoliv dalších licencí, podlicencí ani sekundárních podlicencí pro Objednatele.

1.4 Zajištění servisní podpory Služby

Komunikačním kanálem pro hlášení incidentů a požadavků určenými pracovníky Objednatele je Service Desk Poskytovatele (dále jako „Service Desk"). Service Desk je dostupný v režimu 24x7.

ServiceDesk je pracoviště Poskytovatele přijímající servisní hlášení od určených osob Objednatele zadáním požadavku v aplikaci, telefonicky nebo e-mailem. V případě vzniku incidentu, vzniku požadavku na konfigurační úpravu Služby nepřesahující parametrický rámec tohoto katalogového listu a na konzultace ke Službě, jsou k dispozici následující kontakty Poskytovatele:

- aplikace: https://servicedesk.spcss.cz/
- telefon: [redacted]
- e-mail: [redacted]

Plnění smluvních SLA parametrů Služby souvisejících s řešením incidentů bude vyhodnocováno na základě údajů zaznamenaných v Service Desku.

Servisní podpora bude primárně zajišťovaná prostřednictvím pracovníků Poskytovatele nebo jeho dodavatelů na základě smluv uzavřených mezi Poskytovatelem a jeho servisními dodavateli.

1.5 Kvalitativní parametry Služby

Veškeré parametry specifikované v odstavci 1.5 této přílohy budou specifikovány v dokumentu High level design a následně uvedeny v konkrétní Nabídce a navazující Objednávce.

1.5.1 Odstraňování závad (incident)

Závada je neplánované přerušení nebo zhoršení kvality Služby. Z pohledu závažnosti se závady dělí na následující kategorie:

- Kritická – závada, při níž není Služba použitelná ve svých základních funkcích nebo je zcela nefunkční;
- Závažná – závada, kdy je Služba ve svých funkcích degradovaná natolik, že tento stav omezuje její běžné používání;
- Nezávažná – drobná závada, která nijak významně neovlivňuje Službu.

Požadované lhůty pro Odstranění závady jsou uvedeny v následující tabulce

Lhůta pro Odstranění závady			
Kategorie závady	**Kritická (A)**	**Závažná (B)**	**Nezávažná (C)**
Popis SLA	5 pracovních dnů v týdnu, 8 hodin denně v době od 8:00 do 16:00 hodin, s povinností oznámit zahájení řešení do 30 minut od nahlášení a odstranit závadu do 4 hodin od nahlášení Servisního hlášení.	5 pracovních dnů v týdnu, 8 hodin denně v době od 8:00 do 16:00 hodin, s povinností oznámit zahájení řešení do 1 hodiny od nahlášení a odstranit závadu do 8 hodin od nahlášení Servisního hlášení.	5 pracovních dnů v týdnu, 8 hodin denně v době od 8:00 do 16:00 hodin, s povinností oznámit zahájení řešení nejpozději následující pracovní den a odstranit závadu do 40 hodin od nahlášení Servisního hlášení.

Provozní doba (dny)	5 pracovních dnů v týdnu	5 pracovních dnů v týdnu	5 pracovních dnů v týdnu
Provozní doba (hodiny)	8:00 – 16:00	8:00 – 16:00	8:00 – 16:00
Výjimky z provozní doby	nejsou	nejsou	nejsou
Garantovaný čas reakce operátora	30 minut	30 minut	120 minut
Garantovaný čas zahájení prací na odstranění závady	+45 minut	+1 hodina	následující pracovní den

Požadované lhůty pro obnovení služby dle kategorií závad

Prostředí*	**Lhůta pro obnovení služby v hodinách v provozní době**		
	Závada kategorie Kritická (A)	**Incident kategorie Závažná (B)**	**Incident kategorie Nezávažná (C)**
Vývojové	Dle HLD	Dle HLD	Dle HLD
Produktivní	Dle HLD	Dle HLD	Dle HLD
Testovací	Dle HLD	Dle HLD	Dle HLD

*) konkrétní typy prostředí budou specifikovány dle High level designu

1.5.2 Řešení provozních požadavků (požadavek)

Požadované lhůty pro Řešení provozních požadavků jsou uvedeny v následující tabulce

Lhůta pro Řešení provozních požadavků	
Popis SLA	5 pracovních dnů v týdnu, 8 hodin denně v době od 8:00 do 16:00 hodin.
Provozní doba (dny)	5 pracovních dnů v týdnu
Provozní doba (hodiny)	8:00 – 16:00
Výjimky z provozní doby	nejsou
Garantovaný čas zahájení řešení požadavku	2 hodiny
Garantovaný čas vyřešení požadavku	N/A*)

*) Termín vyřešení se odvíjí od výsledku analýzy požadavku

1.5.3 Roční dostupnost Služby

Požadavek na roční dostupnost Služby podle tohoto katalogového listu je specifikován dle High level designu, a to dle typu prostředí v % v každém kalendářním roce. Požadovaná roční dostupnost ve výše uvedených provozních dobách se posuzuje vždy pro aktuální kalendářní rok. Na počátku každého kalendářního roku Poskytovatel vypočítá maximální možné trvání nedostupnosti Služby pro dané období podle uvedených procentuálních hodnot požadované roční dostupnosti. Provozní požadavky nejsou součástí výše uvedené roční dostupnosti.

1.5.4 Plánované odstávky

V rámci poskytování Služby si Poskytovatel vyhrazuje právo na plánované odstávky celého nebo částí systému. Nedostupnost Služby v době plánovaných odstávek se nezapočítává do celkové roční nedostupnosti Služby.

Doba odstávky, která byla předem řádně ohlášena se nezapočítává do nedostupnosti Služby. Za ohlášení se považuje informování Objednatele e-mailem na adresu Oprávněné osoby Objednatele a to minimálně 48 hodin před zahájením odstávky. Objednatel následně vyslovuje souhlas s navrženou odstávkou, a to do 24 hodin před termínem odstávky. Ovlivnění chodu Služby ze strany Objednatele se nezapočítává do nedostupnosti Služby. V případě urgentní odstávky může být ohlášení jednostranné.

1.5.5 Definice měření dostupnosti

Dostupnost Služby je definovaná při splnění následující podmínky:

- přenosová trasa je funkční, poskytování Služby není výrazně omezeno, ztíženo nebo přerušeno

Za nahlášení nedostupnosti Služby se považuje založení odpovídajícího servisního hlášení dle postupu uvedeného v kapitole 1.4.

Dostupnost služby se vypočítá podle následujícího vzorce:

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

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 plánované odstávky.

1.5.6 Nedodržení kvalitativního parametru Služby

V případě, že ze strany Poskytovatele dojde k nedodržení kvalitativního parametru Služby a pokud se Poskytovatel s Objednatelem nedohodnou jinak, Objednateli vzniká právo na uplatnění smluvní pokuty.

Poskytovatel bude zproštěn povinnosti dodržet kvalitativní parametr Služby, pokud:

- Objednatel prokazatelně neposkytne požadovanou součinnost;
- k nedostupnosti nebo závadě dojde ze strany Objednatele mimo působnost Poskytovatele;
- k nedostupnosti došlo mimo infrastrukturu Poskytovatele;
- vyskytnou se okolnosti, které představují událost vyšší moci.

1.6 Cena za Službu

1.6.1 Příprava Služby

Poskytování Služby bude předcházet příprava, resp. Projektové zřízení Služby. Součástí přípravy jsou kroky konfigurace infrastruktury dle specifikace a zajištění přístupu určeným pracovníkům Objednatele k infrastrukturním zdrojům a případná nezbytná součinnost Poskytovatele Objednateli při spuštění Služby. Cena za přípravu Služby a způsob její fakturace bude uvedena do konkrétní Nabídky a následné Objednávky na základě specifikace v dokumentu High level design.

Příprava	Cena v Kč bez DPH	DPH	Cena v Kč včetně DPH
Celková cena za přípravu	***Výše bude stanovena dle HLD***		

1.6.2 Měsíční cena za Službu

Dále uvedená měsíční cena Služby odpovídá rozsahu specifikovanému v odstavci 1.3 této přílohy. Paušální měsíční cena za Službu a způsob její fakturace bude uveden do konkrétní Nabídky a následné Objednávky na základě specifikace v dokumentu High level design:

Služba	Cena v Kč bez DPH za měsíc	DPH	Cena v Kč včetně DPH za měsíc
Celková měsíční cena Služby	***Dle zadání v dokumentu High level design***		

1.7 Smluvní pokuty za nesplnění parametrů poskytování Služby

Za porušení kvalitativních parametrů, nedodržení požadované lhůty pro odstranění závady ve lhůtě dle odst. 1.5.1 tohoto katalogového listu je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu za každou započatou hodinu prodlení dle následující tabulky.

Za porušení parametru nedodržení požadované roční dostupnosti Služby dle odstavce 1.5.3 tohoto katalogového listu je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu za každou 1 hodinu nedostupnosti Služby nad stanovený limit dle následující tabulky.

Název parametru	Smluvní pokuta za porušení parametru Služby v % z celkové měsíční ceny Služby bez DPH dle odst. 1.5.1 tohoto KL	Max. výše smluvní pokuty v % z celkové měsíční ceny Služby bez DPH dle odst. 1.5.1 tohoto KL	Způsob výpočtu
Dostupnost oblasti Služby	1	40	Za každou započatou hodinu nad povolený limit nedostupnosti nebo doby odstranění závady (incidentu)
Doba odstranění závady (incidentu) kategorie A	1	40	
Doba odstranění závady (incidentu) kategorie B	0,5	15	

Doba odstranění závady (incidentu) kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období, avšak je omezená do výše 50 % ceny Služeb uzavřených Objednávek dle tohoto katalogového listu.

Smluvní pokuty, jejich výše a parametry, pokud budou odlišné od tohoto katalogového listu, budou stanoveny v konkrétní Nabídce a následné Objednávce.

KATALOGOVÝ LIST Č. 11
Služby PaaS pro IS s provozní podporou 24x7

Obsahem katalogového listu je poskytnutí infrastruktury a souvisejících služeb SPCSS (dále jako „Poskytovatel") v úrovni PaaS pro IS jehož provozní doba je 24x7 (dále jen jako „Služba") pro Ministerstvo zahraničních věcí (dále jako „Objednatel").

Čerpané infrastrukturní zdroje pro Službu jsou uvedeny v oboustranně odsouhlasené dokumentaci – High-level design.

1 SLUŽBA PAAS PRO IS S PROVOZNÍ PODPOROU 24X7

1.1 Období poskytování Služby

Služba je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby.

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

1.2 Režim poskytování Služby

Služba dle čl. 1 tohoto katalogového listu bude poskytována v režimu:

Režim poskytování Služby	Doba poskytování
Provozní doba Služby	24x7
Provozní doba podpory Service Desk	24x7

*) režim poskytování Služby bude stanoven v High level designu a následně uveden v konkrétní Nabídce a navazující Objednávce

1.3 Popis rozsahu Služby

Služba bude poskytována dle rozsahu uvedeném v dokumentu High level design pro konkrétní Nabídku a navazující Objednávku. Přehled možného rozsahu služeb:

- Poskytování výpočetního výkonu a zálohovacích kapacit a dalších provozních služeb
- Poskytování správy operačních systémů (dále jako „OS") jejíž součástí jsou následující provozní činnosti:

- Instalace operačních systémů
- Instalace verzí/patchů OS v pravidelných intervalech
- Změny konfigurací OS
- Instalace kritických oprav OS
- Kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz
- Vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu)
- Profylaxe systému dle harmonogramu v měsíčních intervalech
- Instalace a konfigurace nového software
- Instalace a údržba ovladačů a firmware hardware virtualizační platformy Poskytovatele
- Správa účtů v OS
- Úpravy výkonnostních parametrů systému
- Správa souborového systému (filesystem, přístupová práva, kvóty a limity jeho použití)
- Konzultace při poskytování podpory uživatelům
- Údržba dokumentace o konfiguraci OS
- Troubleshooting OS
- Hardening OS
- Testování změn provedených v OS
- Komunikace a řešení problémů s externím suportem
- Konfigurace a nastavení firewallu a antiviru v prostředí OS

- Poskytování správy databáze (dále jako „DB“) jejíž součástí jsou následující provozní činnosti:
  - Instalace databázového serveru bez poskytnutí licence
  - Administrace databáze (změny konfigurací databáze, správa účtů v databázi)
  - Instalace patchů
  - Instalace kritických oprav
  - Instalace security patchů
  - Upgrade a migrace databáze
  - Definice zálohování a obnovy dat
  - Vytvoření a správa replikací
  - Vyhodnocování výstupů z monitoringu databáze (sledování výkonnostních parametrů a zatížení databáze)
  - Úpravy výkonnostních parametrů databáze
  - Reportování výstupů z monitoringu na vyžádání
  - Preventivní údržba databázového serveru a databází
  - Restarty databází dle požadavků Objednatele
  - Odpovídání na technické dotazy Objednateli
  - Údržba dokumentace o konfiguraci databáze

  - Troubleshooting databáze
  - Testování změn provedených v databázi
  - Komunikace a řešení problémů s externím suportem

- Poskytování bezpečného komunikačního rozhraní:
  - Zajištění komunikační infrastruktury dle KL – Landing zóna – MZV

- Řízení provozu a dohled nad kvalitou poskytované Služby:
  - Provozní monitoring infrastruktury a platforem
  - Uchování provozních logů
  - Zálohování infrastruktury a platforem do úložišť v prostředí Poskytovatele
  - Řízení provozu Služby dle dle ISO standardů (ČSN ISO/IEC 20000-1:2019, ČSN EN ISO 9001:2016)
  - Projektové a organizační řízení služby na straně Poskytovatele během přípravy a následného provozu Služby

- Bezpečnost:
  - Zajištění trvalého bezpečnostního monitoringu infrastrukturních komponent Služby, a to dle ZoKB a VoKB

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

- Požadované součinnosti poskytované Objednatelem:
  - Objednatel zajistí na své straně nominaci odpovědných osob za účelem projektového řízení a odpovídající technické role pro období implementace služby do prostředí Poskytovatele infrastruktury
  - Objednatel se zavazuje poskytnout nezbytné osobní údaje určené pro zajištění VPN přístupu určeným pracovníkům Objednatele do prostředí Poskytovatele.

V termínu zahájení poskytování Služby podle tohoto katalogového listu má Objednatel vybudované prostředí pro provoz IS v objemu a nastavení uvedených v dokumentu High-level design.

Součástí ceny jsou licence OS výrobce, dle požadavků specifikovaných v dokumentu High level design.

Součástí ceny nejsou licence MS SQL databází.

Součástí Služby není poskytnutí jakýchkoliv dalších licencí, podlicencí ani sekundárních podlicencí pro Objednatele.

1.4 Zajištění servisní podpory Služby

Komunikačním kanálem pro hlášení incidentů a požadavků určenými pracovníky Objednatele je Service Desk Poskytovatele (dále jako „Service Desk"). Service Desk je dostupný v režimu 24x7.

ServiceDesk je pracoviště Poskytovatele přijímající servisní hlášení od určených osob Objednatele zadáním požadavku v aplikaci, telefonicky nebo e-mailem. V případě vzniku incidentu, vzniku požadavku na konfigurační úpravu Služby nepřesahující parametrický rámec tohoto katalogového listu a na konzultace ke Službě, jsou k dispozici následující kontakty Poskytovatele:

- aplikace: https://servicedesk.spcss.cz/
- telefon: [redacted]
- e-mail: [redacted]

Plnění smluvních SLA parametrů Služby souvisejících s řešením incidentů bude vyhodnocováno na základě údajů zaznamenaných v Service Desku.

Servisní podpora bude primárně zajišťovaná prostřednictvím pracovníků Poskytovatele nebo jeho dodavatelů na základě smluv uzavřených mezi Poskytovatelem a jeho servisními dodavateli.

1.5 Kvalitativní parametry Služby

Veškeré parametry specifikované v odstavci 1.5 této přílohy budou specifikovány v dokumentu High level design a následně uvedeny v konkrétní Nabídce a navazující Objednávce.

1.5.1 Odstraňování závad (incident)

Závada je neplánované přerušení nebo zhoršení kvality Služby. Z pohledu závažnosti se závady dělí na následující kategorie:

- Kritická – závada, při níž není Služba použitelná ve svých základních funkcích nebo je zcela nefunkční;
- Závažná – závada, kdy je Služba ve svých funkcích degradovaná natolik, že tento stav omezuje její běžné používání;
- Nezávažná – drobná závada, která nijak významně neovlivňuje Službu.

Požadované lhůty pro Odstranění závady jsou uvedeny v následující tabulce

Lhůta pro Odstranění závady			
Kategorie závady	**Kritická (A)**	**Závažná (B)**	**Nezávažná (C)**
Popis SLA	7 dnů v týdnu, 24 hodin denně v době od 0:00 do 24:00 hodin, s povinností	7 dnů v týdnu, 13 hodin denně v době od 7:00 do 20:00 hodin, s	5 pracovních dnů v týdnu, 11 hodin denně v době od 7:00 do 18:00 hodin,

Lhůta pro Odstranění závady			
Kategorie závady	**Kritická (A)**	**Závažná (B)**	**Nezávažná (C)**
	oznámit zahájení řešení do 15 minut od nahlášení a odstranit závadu do 4 hodin od nahlášení Servisního hlášení.	povinností oznámit zahájení řešení do 1 hodiny od nahlášení a odstranit závadu do 8 hodin od nahlášení Servisního hlášení.	s povinností oznámit zahájení řešení nejpozději následující pracovní den a odstranit závadu do 40 hodin od nahlášení Servisního hlášení.
Provozní doba (dny)	7 dnů v týdnu	7 dnů v týdnu	5 pracovních dnů v týdnu
Provozní doba (hodiny)	Nepřetržitě	7:00 – 20:00	7:00 – 18:00
Výjimky z provozní doby	nejsou	nejsou	nejsou
Garantovaný čas reakce operátora	15 minut	30 minut	120 minut
Garantovaný čas zahájení prací na odstranění závady	+30 minut	+45 minut	+8 hodin

Požadované lhůty pro obnovení služby dle kategorií závad:

Prostředí*	**Lhůta pro obnovení služby v hodinách v provozní době**		
	Závada kategorie Kritická (A)	**Incident kategorie Závažná (B)**	**Incident kategorie Nezávažná (C)**
Produktivní	Dle HLD	Dle HLD	Dle HLD
Testovací	Dle HLD	Dle HLD	Dle HLD
Vývojové	Dle HLD	Dle HLD	Dle HLD

*) konkrétní typy prostředí budou specifikovány dle dokumentu High level design

1.5.2 Řešení provozních požadavků (požadavek)

Požadované lhůty pro Řešení provozních požadavků jsou uvedeny v následující tabulce:

Lhůta pro Řešení provozních požadavků	
Popis SLA	5 pracovních dnů v týdnu, 13 hodin denně v době od 7:00 do 20:00 hodin

Provozní doba (dny)	5 pracovních dnů v týdnu
Provozní doba (hodiny)	7:00 – 20:00
Výjimky z provozní doby	nejsou
Garantovaný čas zahájení řešení požadavku	2 hodiny
Garantovaný čas vyřešení požadavku	N/A*)

*) Termín vyřešení se odvíjí od výsledku analýzy požadavku

1.5.3 Roční dostupnost Služby

Požadavek na roční dostupnost Služby podle tohoto katalogového listu je specifikován dle High level designu, a to dle typu prostředí v % v každém kalendářním roce. Požadovaná roční dostupnost ve výše uvedených provozních dobách se posuzuje vždy pro aktuální kalendářní rok. Na počátku každého kalendářního roku Poskytovatel vypočítá maximální možné trvání nedostupnosti Služby pro dané období podle uvedených procentuálních hodnot požadované roční dostupnosti. Provozní požadavky nejsou součástí výše uvedené roční dostupnosti.

1.5.4 Plánované odstávky

V rámci poskytování Služby si Poskytovatel vyhrazuje právo na plánované odstávky celého nebo částí systému. Nedostupnost Služby v době plánovaných odstávek se nezapočítává do celkové roční nedostupnosti Služby.

Doba odstávky, která byla předem řádně ohlášena se nezapočítává do nedostupnosti Služby. Za ohlášení se považuje informování Objednatele e-mailem na adresu Oprávněné osoby Objednatele a to minimálně 48 hodin před zahájením odstávky. Objednatel následně vyslovuje souhlas s navrženou odstávkou, a to do 24 hodin před termínem odstávky. Ovlivnění chodu Služby ze strany Objednatele se nezapočítává do nedostupnosti Služby. V případě urgentní odstávky může být ohlášení jednostranné.

1.5.5 Definice měření dostupnosti

Dostupnost Služby je definovaná při splnění následující podmínky:

- přenosová trasa je funkční, poskytování Služby není výrazně omezeno, ztíženo nebo přerušeno

Za nahlášení nedostupnosti Služby se považuje založení odpovídajícího servisního hlášení dle postupu uvedeného v kapitole 1.4.

Dostupnost služby se vypočítá podle následujícího vzorce:

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

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 plánované odstávky.

1.5.6 Nedodržení kvalitativního parametru Služby

V případě, že ze strany Poskytovatele dojde k nedodržení kvalitativního parametru Služby a pokud se Poskytovatel s Objednatelem nedohodnou jinak, Objednateli vzniká právo na uplatnění smluvní pokuty.

Poskytovatel bude zproštěn povinnosti dodržet kvalitativní parametr Služby, pokud:

- Objednatel prokazatelně neposkytne požadovanou součinnost;
- k nedostupnosti nebo závadě dojde ze strany Objednatele mimo působnost Poskytovatele;
- k nedostupnosti došlo mimo infrastrukturu Poskytovatele;
- vyskytnou se okolnosti, které představují událost vyšší moci.

1.6 Cena za Službu

1.6.1 Příprava Služby

Poskytování Služby bude předcházet příprava, resp. Projektové zřízení Služby. Součástí přípravy jsou kroky konfigurace infrastruktury dle specifikace a zajištění přístupu určeným pracovníkům Objednatele k infrastrukturním zdrojům a případná nezbytná součinnost Poskytovatele Objednateli při spuštění Služby. Cena za přípravu Služby a způsob její fakturace bude uvedena do konkrétní Nabídky a následné Objednávky na základě specifikace v dokumentu High level design.

Příprava	Cena v Kč bez DPH	DPH	Cena v Kč včetně DPH
Celková cena za přípravu	***Výše bude stanovena dle HLD***		

1.6.2 Měsíční cena za Službu

Uvedená měsíční cena Služby odpovídá rozsahu specifikovanému v odstavci 1.3 této přílohy. Paušální měsíční cena za Službu a způsob její fakturace bude uveden do konkrétní Nabídky a následné Objednávky na základě specifikace v dokumentu High level design:

Služba	Cena v Kč bez DPH za měsíc	DPH	Cena v Kč včetně DPH za měsíc
Celková měsíční cena Služby	***Dle zadání v dokumentu High level design***		

1.7 Smluvní pokuty za nesplnění parametrů poskytování Služby

Za porušení kvalitativních parametrů, nedodržení požadované lhůty pro odstranění závady ve lhůtě dle odst. 1.5.1 tohoto katalogového listu je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu za každou započatou hodinu prodlení dle následující tabulky.

Za porušení parametru nedodržení požadované roční dostupnosti Služby dle odstavce 1.5.3 tohoto katalogového listu je Objednatel oprávněn uplatnit vůči Poskytovateli smluvní pokutu za každou 1 hodinu nedostupnosti Služby nad stanovený limit dle následující tabulky.

Název parametru	Smluvní pokuta za porušení parametru Služby v % z celkové měsíční ceny Služby bez DPH dle odst. 1.5.1 tohoto KL	Max. výše smluvní pokuty v % z celkové měsíční ceny Služby bez DPH dle odst. 1.5.1 tohoto KL	Způsob výpočtu
Dostupnost oblasti Služby	1	40	Za každou započatou hodinu nad povolený limit nedostupnosti nebo doby odstranění závady (incidentu)
Doba odstranění závady (incidentu) kategorie A	1	40	
Doba odstranění závady (incidentu) kategorie B	0,5	15	
Doba odstranění závady (incidentu) kategorie C	0,1	2,5	

Maximální výše smluvní pokuty se vztahuje na součet smluvních pokut za nesplnění všech SLA u každého jednotlivého parametru za dané vyhodnocovací období, avšak je omezená do výše 50 % ceny Služeb uzavřených Objednávek dle tohoto katalogového listu.

Smluvní pokuty, jejich výše a parametry, pokud budou odlišné od tohoto katalogového listu, budou stanoveny v konkrétní Nabídce a následné Objednávce.

Odborné role SPCSS

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.

SPCSS
Státní pokladna
Centrum sdílených služeb

ID	Název Odborné role	Popis činností
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 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.

ID	Název Odborné role	Popis činností
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 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

ID	Název Odborné role	Popis činností
		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 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

ID	Název Odborné role	Popis činností
		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.

Další odborné role

ID	Název Odborné role	Popis činností
23	Tester junior	Připravuje nebo se podílí na přípravě testů (Test Cases, Test Scripts) a testovacích dat ve spolupráci s analytickým nebo implementačním týmem. Pracuje v projektovém týmu na externím či interním projektu Zadavatele jako specialista zodpovědný za testování dodávaného řešení. Provádí ověření funkčnosti dodávaného řešení dle zadání a reportuje případné chyby a nedostatky. Podílí se na přípravě a realizaci automatizovaných a/nebo performance testů. Na základě průběhů nebo výstupů testování navrhuje optimalizaci uživatelského rozhraní.
24	Tester analytik	Připravuje nebo se podílí na přípravě testů (Test Cases, Test Scripts) a testovacích dat ve spolupráci s analytickým nebo implementačním týmem. Zodpovídá za stanovení strategie přípravy a struktury testovacích scénářů, navrhuje strategii a plán testování. Podílí se na přípravě automatizovaných a/nebo performance testů. Na základě průběhů nebo výstupů navrhuje optimalizaci uživatelského rozhraní. Spolupracuje na presale aktivitách, vyhodnocování obchodních příležitostí (poptávek) a přípravách částí nabídek zejména v oblasti testování.
25	Tester senior	Připravuje nebo se podílí na přípravě testů (Test Cases, Test Scripts) a testovacích dat ve spolupráci s analytickým nebo implementačním týmem. Zodpovídá za stanovení strategie přípravy a struktury testovacích scénářů. Pracuje v projektovém týmu na externím či interním projektu jako specialista zodpovědný za testování dodávaného řešení. Provádí ověření funkčnosti dodávaného řešení dle zadání a reportuje případné chyby a nedostatky. Podílí se na přípravě a realizaci automatizovaných a/nebo performance testů. Na základě průběhů nebo výstupů navrhuje optimalizaci uživatelského rozhraní. Zodpovídá jako člen projektového týmu v pozici test manažera za stanovení strategie a plánu testování a za pravidelný reporting PM o stavu testování a nalezených/opravených vadách. Koordinuje činnosti týmu testerů projektu (interních i externích). Kontroluje kvalitu dodávek poddodavatelů Zadavatele a komunikuje s nimi v návaznosti na výstupy/závěry testování oblasti technických řešení. Spolupracuje se zákazníkem Zadavatele v technických oblastech testování, součiní s vývojovým týmem při vývoji SW řešení

ID	Název Odborné role	Popis činností
		a spolupracuje při analýze zjištěných vad. Spolupracuje na presale aktivitách, vyhodnocování obchodních příležitostí (poptávek) a přípravách částí nabídek zejména v oblasti testování.Podílí se na školení, kontrole a odborném dohledu činností junior testerů.
26	Tester senior – automatizace	Připravuje nebo se podílí na přípravě testů (Test Cases, Test Scripts) a testovacích dat ve spolupráci s analytickým nebo implementačním týmem. Zodpovídá za stanovení strategie přípravy a struktury testovacích scénářů, navrhuje strategii a plán testování. Pracuje v projektovém týmu na externím či interním projektu jako specialista zodpovědný za testování dodávaného řešení. Provádí ověření funkčnosti dodávaného řešení dle zadání a reportuje případné chyby a nedostatky. Podílí se na přípravě a realizaci automatizovaných a/nebo performance testů. Na základě průběhů nebo výstupů navrhuje optimalizaci uživatelského rozhraní. Zodpovídá jako člen projektového týmu v pozici test manažera za stanovení strategie a plánu testování a za pravidelný reporting PM o stavu testování a nalezených/opravených vadách. Koordinuje činnosti týmu testerů projektu (interních i externích). Kontroluje kvalitu dodávek poddodavatelů Zadavatele a komunikuje s nimi v návaznosti na výstupy/závěry testování oblasti technických řešení. Spolupracuje se zákazníkem Zadavatele v technických oblastech testování, součiní s vývojovým týmem při vývoji SW řešení a spolupracuje při analýze zjištěných vad. Spolupracuje na presale aktivitách, vyhodnocování obchodních příležitostí (poptávek) a přípravách částí nabídek zejména v oblasti testování. Podílí se na školení, kontrole a odborném dohledu činností junior testerů.
27	Tester senior – mobilní aplikace	Připravuje nebo se podílí na přípravě testů (Test Cases, Test Scripts) a testovacích dat ve spolupráci s analytickým nebo implementačním týmem. Zodpovídá za stanovení strategie přípravy a struktury testovacích scénářů, navrhuje strategii a plán testování. Pracuje v projektovém týmu na externím či interním projektu jako specialista zodpovědný za testování dodávaného řešení. Provádí ověření funkčnosti dodávaného řešení dle zadání a reportuje případné chyby a nedostatky. Podílí se na přípravě a realizaci automatizovaných a/nebo performance testů. Na základě průběhů nebo výstupů navrhuje optimalizaci uživatelského rozhraní. Zodpovídá jako člen projektového týmu v pozici test manažera za stanovení strategie a plánu testování a za pravidelný reporting PM o stavu testování a nalezených/opravených vadách. Koordinuje činnosti týmu testerů projektu (interních i externích). Kontroluje kvalitu dodávek poddodavatelů Zadavatele a komunikuje s nimi v návaznosti na výstupy/závěry testování oblasti technických řešení. Spolupracuje se zákazníkem Zadavatele v technických oblastech testování, součiní s vývojovým týmem při vývoji SW řešení a spolupracuje při analýze zjištěných vad. Spolupracuje na presale aktivitách, vyhodnocování obchodních příležitostí (poptávek) a přípravách částí nabídek zejména v oblasti testování. Podílí se na školení, kontrole a odborném dohledu činností junior testerů.
28	DevOps engineer junior	Připravuje (kompilace, provisioning, nastavení) nástroje pro vývoj IT řešení se zaměřením na cloud nativ aplikace. Připravuje infrastruktury pro celý životní cyklus IT řešení se zaměřením na "infrastructure as a code" v privátním a public cloudu. Zajišťuje zlepšování a automatizace release procesů. Zajišťuje porozumění potřebám zainteresovaných stran v projektech a tlumočení těchto potřeb vývojářům. Testuje a kontroluje zdrojové kódy, vč. analýzy výsledků testování (z pohledu dopadů na výkon a bezpečnost infrastruktury). Navrhuje, řeší a kontroluje bezpečnosti a odolnosti IT řešení proti bezpečnostním hrozbám. Identifikuje technické problémy a jejich vyřešení. Vyvíjí částí SW. Spolupracuje s vývojáři, testery a realizačním týmem na

ID	Název Odborné role	Popis činností
		zajištění vývoje v kontextu kontinuální integrace a nasazení řešení. Spolupracuje na vytvoření plánů projektů.
29	DevOps engineer senior	Připravuje (kompilace, provisioning, nastavení) nástroje pro vývoj IT řešení se zaměřením na cloud nativ aplikace. Připravuje infrastruktury pro celý životní cyklus IT řešení se zaměřením na "infrastructure as a code" v privátním a public cloudu. Zajišťuje zlepšování a automatizace release procesů. Zajišťuje porozumění potřebám zainteresovaných stran v projektech a tlumočit tyto potřeby vývojářům. Testuje a kontroluje zdrojové kódy, vč. analýzy výsledků testování (z pohledu dopadů na výkon a bezpečnost infrastruktury). Navrhuje, řeší a kontroluje bezpečnosti a odolnosti IT řešení proti bezpečnostním hrozbám. Identifikuje technické problémy a řídí jejich vyřešení. Spolupracuje s vývojáři, testery a realizačním týmem na zajištění vývoje v kontextu kontinuální integrace a nasazení řešení. Spolupracuje na vytvoření plánů projektů a součiní při rozhodovacích procesech projektů.
30	Datový architekt	Navrhuje datové modely pro vysoce dostupná o odolná databázová a aplikační prostředí (včetně business critical systémů). Vytváří a poskytuje funkční rámce pro implementaci postupů správy podnikových dat, vč. postupů, metod a technik, funkcí, rolí, výstupů a metrik. Navrhuje, připravuje a kontroluje migrační scénáře dat mezi různými prostředími a databázemi. Provádí analýzu, návrh a dohled nad implementací navrženého řešení ve svěřené oblasti.
31	Databázový architekt	Vytváří analýzy, návrhy a zajišťuje dohled nad implementací architektury databázových řešení s vysokou dostupností. Navrhuje, připravuje a kontroluje migrační scénáře dat mezi různými prostředími a databázemi. Provádí analýzu, návrh a dohled nad implementací navrženého řešení ve svěřené oblasti.
32	System architect / Infrastrukturní systémový architekt	Odpovídá za analýzu, návrh, implementaci, správu, zabezpečení, údržbu a podporu prostředí založeného na platformě Windows Server / Active Directory. Zajišťuje prostředí, které se skládá z infrastruktury: Active Directory, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL Services, Azure Active Directory, služby souborů a tisku, systémy WSUS, virtualizace. Navrhuje a vykonává postupy pro práci s nástroji pro správu výkonu systémů a správu infrastruktury. Navrhuje a kontroluje bezpečnostní metodiky, metodiky virtualizace, metodiky vysoké dostupnosti a zotavení po katastrofě. Navrhuje řešení a realizaci systému s vysokou dostupnosti.
33	Enterprise Architekt	Řídí vytvoření a optimalizaci návrhu architektury ICT systémů. Zodpovídá za dohled, zlepšování a upgrade podnikových služeb, SW i HW. Navrhuje High-level architekturu napříč systémy, vč. jejich využití dle různých pohledů. Zajišťuje a odpovídá za správu podnikových dat, zajišťuje modelování v Archimate / TOGAF. Spolupracuje při tvorbě obchodní strategie. Navrhuje a realizuje procesy související se službami poskytovanými s využitím cloud computing, spolupracuje při návrhu architektura systémů, strategií a podnikových řešení.
34	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

ID	Název Odborné role	Popis činností
		místa v projektu. Spolupracuje při přípravě návrhu nabídky pro požadované řešení zákazníka.
35	Projektový administrátor/koordinátor	Zajišťuje administrativní podporu projektového manažera. Udržuje vybrané projektové dokumentace (např. registr rizik/problémů, seznam úkolů), vč. ukládání projektové dokumenty na projektový web a do spisové služby. Zajišťuje schvalování projektových dokumentů. Vytváří a distribuuje zápisy z porad, připravuje podklady k jednání podle pokynů projektového manažera, kontroluje plnění úkolů. Připravuje zprávu o stavu projektu, vytváří pravidelné a ad-hoc reporty a zprávy dle potřeb projektového manažera. Kontroluje náklady projektu.
36	ICT Business Analytik junior	Zajišťuje analytické činnosti z pohledu businessu i ICT. Provádí sběr požadavků zákazníka/uživatele a jejich analýzu, vytváří a udržuje katalog požadavků. Spolupracuje se zákazníkem/uživatelem při definování požadovaného řešení. Spolupracuje na návrhu a prezentaci analytického řešení (apod.) pro koncové uživatele. Komunikuje vytvořené analytické podklady s dalšími členy projektových a realizačních týmů. Zajišťuje rozpracování/detailizaci analytických podkladů na základě požadavků spolupracujících rolí/členů týmů (architekti, vývojáři, testeři). Podílí se na přípravě uživatelské a technické dokumentace.
37	ICT Business Analytik (UML, BPMN) senior	Zajišťuje analytické činnosti z pohledu businessu i ICT. Provádí sběr požadavků zákazníka/uživatele a jejich analýzu, vytváří a udržuje katalog požadavků. Spolupracuje se zákazníkem/uživatelem při definování požadovaného řešení. Připravuje časový odhad náročnosti zpracování daného analytického řešení. Spolupracuje na návrhu a prezentaci analytického řešení (návrh datového modelu, procesní modely, UC diagramy apod.) pro koncové uživatele. Zodpovídá za zpracování návrhu analytického řešení a za použití jednotné metodiky. Prezentuje a obhajuje návrh analytického řešení vůči zákazníkovi/uživateli. Koordinuje činnosti vykonávané podřazenými analytickými Odborná rolemi v rámci týmů. Komunikuje vytvořené analytické podklady s dalšími členy projektových a realizačních týmů. Podílí se na přípravě obchodní a technické dokumentace.
38	ICT Business Analytik (Archimate) junior	Zajišťuje analytické činnosti z pohledu businessu i ICT. Provádí sběr požadavků zákazníka/uživatele a jejich analýzu, vytváří a udržuje katalog požadavků. Spolupracuje se zákazníkem/uživatelem při definování požadovaného řešení. Spolupracuje na návrhu a prezentaci analytického řešení (návrh datového modelu, procesní modely, UC diagramy apod.) pro koncové uživatele. Komunikuje vytvořené analytické podklady s dalšími členy projektových a realizačních týmů. Zajišťuje rozpracování/detailizaci analytických podkladů na základě požadavků spolupracujících rolí/členů týmů (architekti, vývojáři, testeři). Podílí se na přípravě uživatelské a technické dokumentace.
39	ICT Business Analytik (Archimate) senior	Zajišťuje analytické činnosti z pohledu businessu i ICT. Provádí sběr požadavků zákazníka/uživatele a jejich analýzu, vytváří a udržuje katalog požadavků. Spolupracuje se zákazníkem/uživatelem při definování požadovaného řešení. Připravuje časový odhad náročnosti zpracování daného analytického řešení. Spolupracuje na návrhu a prezentaci analytického řešení (návrh datového modelu, procesní modely, UC diagramy apod.) pro koncové uživatele. Zodpovídá za zpracování návrhu analytického řešení a za použití jednotné metodiky. Prezentuje a obhajuje návrh analytického řešení vůči zákazníkovi/uživateli. Koordinuje činnosti vykonávané podřazenými analytickými Odborná rolemi v rámci týmů. Komunikuje vytvořené analytické podklady s dalšími členy projektových a realizačních týmů. Podílí se na přípravě obchodní a technické dokumentace.
40	Kotlin Vývojář Backend junior	Realizuje SW vývoj v programovacím jazyce Kotlin. Podílí se na tvorbě designu aplikací a SW aplikační architektuře. Podílí se na přípravě

ID	Název Odborné role	Popis činností
		a aktualizaci vývojářské dokumentace. Zodpovídá za řešení hlášených vad vyvíjeného SW v přidělených částech.
41	Kotlin Vývojář Backend senior	Zajišťuje plnění vývojových úkolů ve stanovených termínech. Odpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech. Navrhuje relační databáze a UML modely pro aplikace. Podílí se na tvorbě designu aplikací a na SW aplikační architektuře. Podílí se na přípravě a aktualizaci vývojářské dokumentace. Podílí se na školení, odborném dohledu a kontrole členů týmu v juniorských pozicích. Provádí SW vývoj v programovacím jazyce Kotlin. Spolupracuje na presale aktivitách, vyhodnocování obchodních příležitostí (poptávek) a přípravách nabídek ve vybraných oblastech.
42	Kotlin Vývojář Frontend junior	Realizuje SW vývoj v programovacím jazyce Kotlin. Podílí se na tvorbě designu aplikací a na SW aplikační architektuře. Podílí se na přípravě a aktualizaci vývojářské dokumentace. Zodpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech.
43	Kotlin Vývojář Frontend senior	Zajišťuje plnění vývojových úkolů ve stanovených termínech. Odpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech. Navrhuje relační databáze a UML modely pro aplikace. Podílí se na tvorbě designu aplikací a na SW aplikační architektuře. Podílí se na přípravě a aktualizaci vývojářské dokumentace. Podílí se na školení, odborné dohledu a kontrole členů týmu v juniorských pozicích. Provádí SW vývoj v programovacím jazyce Kotlin. Spolupracuje na presale aktivitách, vyhodnocování obchodních příležitostí (poptávek) a přípravách nabídek ve vybraných oblastech.
44	Java Vývojář Backend junior	Realizuje SW vývoj v programovacím jazyce Java. Podílí se na tvorbě designu aplikací a na SW aplikační architektuře. Podílí se na přípravě a aktualizaci vývojářské dokumentace. Zodpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech.
45	Java Vývojář Backend senior	Zajišťuje plnění vývojových úkolů ve stanovených termínech. Odpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech. Navrhuje relační databáze a UML modely pro aplikace. Podílí se na tvorbě designu aplikací a na SW aplikační architektuře. Podílí se na přípravě a aktualizaci adekvátní vývojářské dokumentace. Podílí se na kontrole a předávání znalostí členům týmu v juniorských pozicích. Provádí SW vývoj v příslušném programovacím jazyce. Spolupracuje na presale aktivitách, vyhodnocování obchodních příležitostí (poptávek) a přípravách nabídek.
46	Java Vývojář Frontend junior	Realizuje SW vývoj v programovacím jazyce Java. Podílí se na tvorbě designu aplikací a na SW aplikační architektuře. Podílí se na přípravě a aktualizaci vývojářské dokumentace. Zodpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech.
47	Java Vývojář Frontend senior	Zajišťuje plnění vývojových úkolů ve stanovených termínech. Odpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech. Navrhuje relační databáze a UML modely pro aplikace. Podílí se na tvorbě designu aplikací a na SW aplikační architektuře. Podílí se na přípravě a aktualizaci adekvátní vývojářské dokumentace. Podílí se na kontrole a předávání znalostí členům týmu v juniorských pozicích. Provádí SW vývoj v příslušném programovacím jazyce. Spolupracuje na presale aktivitách, vyhodnocování obchodních příležitostí (poptávek) a přípravách nabídek.
48	.NET Vývojář Backend junior	Realizuje SW vývoj v příslušném programovacím jazyce. Podílí se na tvorbě designu aplikací a na SW aplikační architektuře. Podílí se na přípravě a aktualizaci adekvátní vývojářské dokumentace. Zodpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech.
49	.NET Vývojář Backend senior	Zajišťuje plnění vývojových úkolů ve stanovených termínech. Odpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech. Navrhuje relační databáze a UML modely pro aplikace. Podílí se na tvorbě designu aplikací a na SW aplikační architektuře. Podílí se na přípravě a aktualizaci adekvátní vývojářské dokumentace. Podílí se na kontrole a předávání znalostí členům týmu v juniorských pozicích.

ID	Název Odborné role	Popis činností
		Provádí SW vývoj v příslušném programovacím jazyce. Spolupracuje na presale aktivitách, vyhodnocování obchodních příležitostí (poptávek) a přípravách nabídek.
50	.NET Vývojář Frontend junior	Zodpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech. Realizuje SW vývoj v příslušném programovacím jazyce. Podílí se na tvorbě designu aplikací a na SW aplikační architektuře. Podílí se na přípravě a aktualizaci adekvátní vývojářské dokumentace.
51	.NET Vývojář Frontend senior	Zajišťuje plnění vývojových úkolů ve stanovených termínech. Odpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech. Navrhuje relační databáze a UML modely pro aplikace. Podílí se na tvorbě designu aplikací a na SW aplikační architektuře. Podílí se na přípravě a aktualizaci adekvátní vývojářské dokumentace. Podílí se na kontrole a předávání znalostí členům týmu v juniorských pozicích. Provádí SW vývoj v příslušném programovacím jazyce. Spolupracuje na presale aktivitách, vyhodnocování obchodních příležitostí (poptávek) a přípravách nabídek.
52	DB Analytik	Provádí analytické činnosti z pohledu potřeb aplikace, business procesů a ICT prostředků (DB, HW). Provádí výběr vhodných databázových a softwarových prostředků na základě požadavků (business procesy, aplikace, ICT prostředky). Navrhuje a vytváří logické i fyzické databázové modely. Navrhuje a připravuje logické databázové funkce a připravuje podklady pro jejich vývoj. Podílí se na implementaci databázových modelů a schémat.
53	DB Specialista	Provádí konfiguraci daných databázových softwarových prostředků a optimalizuje výkon řešení. Analyzuje výkonnostních problémy a navrhuje jejich řešení. Implementuje, provozuje a dohleduje dané databázové řešení a softwarové prostředky.
54	DB vývojář	Zajišťuje plnění vývojových úkolů / databázových funkcí na základě požadavků od databázového analytika. Navrhuje vhodné softwarové prostředky pro dané technologie / technologické celky. Příprava a realizace automatického testování databázových funkcí / funkcionalit. Zodpovídá za kvalitu zdrojového kódu ve svěřené části. Vytváří a upravuje procedury a funkce, vyhledává data a vytváří dotazy v databázích. Navrhuje optimalizaci databázových objektů a opravuje chyby
55	Metadatový specialista	Analyzuje požadavky na metadata a provádí volbu vhodné technologie. Připravuje zadání pro vývoj a implementaci. Ověřuje správnou funkci metadatových softwarových prostředků a validuje použité metadatové formáty.
56	Specialista integrace senior	Připravuje modely integrací, komunikační schémata a mapování jednotlivých interface, vč. tvorby návrhů řešení. Navrhuje a vytváří definice XML popisující jednotlivé komunikace a transformace (wsdl, xsd). Tvoří technickou analýzu a návrh řešení (nejen) nad integrační platformou společnosti, vč. volby vhodné technologie (ETL, ESB, SOAP, REST). Navrhuje technické integrační patterny, pravidla a použití integračních technologií pro různé situace.
57	DWH architekt	Vytváří analýzy, návrhy a dohlíží nad implementaci řešení pro Business intelligence (BI) a pro datový sklad (DWH). Definuje Extract, transform, load (ETL) procesy, včetně návaznosti a zobrazení dat pomocí prezentační vrstvy realizované systémy PowerBI, Reporting services, Googdata. Navrhuje metodiky přípravy metadat dle různých ETL procesů, včetně definice jejich testů a monitoringu. Analyzuje cíle architektury datového skladu. Vytváří fyzické i logické datové modely a definuje klíčové datové zdroje. Navrhuje a připravuje Online Analytical Processing (OLAP) kostky. Definuje standardy metadat pro datový sklad.
58	Quality assurance manager senior	Zodpovídá za oblast kvality realizovaných řešení. Řízení a zlepšování systému kvality dle norem kvality a oborových standardů. Řídí řešení vzniklých problémů při tvorbě řešení / jednotlivých produktů. Zodpovídá za vedení dokumentace dle norem a potřeb projektů.

ID	Název Odborné role	Popis činností
		Provádí audit v rámci realizovaných řešení. Odpovídá za tvorba podkladů, zpráv a reportů z auditů.
59	Chatbot designer	Navrhuje konverzace a vede konverzaci s chatbotx a hlasovými asistenty. Spolupracuje návrhu na využití chatbotu. Spolupracuje s vývojáři na integraci chatbotu s externími IT systémy, zodpovídá za řešení hlášených vad. Provádí testy, kontroluje použitelnost a optimalizuje provoz chatbotů. Získává distribuované znalosti a procesy zákazníka, aby navrhoval konverzaci. Podílí se na tvorbě a designu řešení, podílí se na přípravě a aktualizaci dokumentace
60	Specialista bezpečnosti – konzultant – Senior	Vykonává Odbornou roli bezpečnostního specialisty na podporu bezpečnostních rolí dle § 6 a 7 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (VoKB) dle jejich pokynů pro systém spravovaný/provozovaný zákazníkem. Podílí se na nastavování a aktualizaci bezpečnostních pravidel, podílí se na kontrole jejich dodržování, podílí se na analýze a návrzích bezpečnostních opatření, a to v rozsahu pokynů udělených rolemi dle § 6 a 7 VokB. Provádí konzultační a poradenskou činnost na základě pokynu rolí dle § 6 a 7 VokB. Připravuje podklady na základě pokynů rolí dle § 6 a 7 VokB zejména v oblasti kybernetické bezpečnosti, business continuity a ochrany osobních údajů ve vztahu ke kybernetické bezpečnosti.
61	Python vývojář junior	Zodpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech. Realizuje SW vývoj v příslušném programovacím jazyce. Podílí se na tvorbě designu aplikací a SW aplikační architektuře. Podílí se na přípravě a aktualizaci adekvátní vývojářské dokumentace.
62	Python vývojář senior	Zajišťuje plnění vývojových úkolů ve stanovených termínech, odpovídá za řešení hlášených vad vyvíjeného SW v jemu přidělených částech. Navrhuje relační databáze a UML modely pro aplikace. Podílí se na tvorbě designu aplikací a SW aplikační architektuře. Podílí se na přípravě a aktualizaci adekvátní vývojářské dokumentace. Podílí se na kontrola a školení juniorských pozic v týmu. Provádí SW vývoj v příslušném programovacím jazyce, podílí se na testování. Spolupracuje na presale aktivitách, vyhodnocování obchodních příležitostí (poptávek) a přípravách nabídek.
63	Cloud architekt	Zpracovává analýzu, návrh a dohled nad implementaci řešení cloudových systémů, včetně návrhu migrace aplikací do cloudu. Tvoří cloudové strategie a spolupracuje na procesu adaptace. Navrhuje vyhodnocování a dohled cloudové aplikace a infrastruktury. Spolupracuje s oddělením bezpečnosti a navrhuje zabezpečení cloudových řešení. Spolupracuje na přípravě nabídek cloud služeb a řešení založených na cloudu zákazníka.
64	Správce identit senior	Nastavuje a konfiguruje procesy nutné ke správnému fungování nástroje pro správu identit a přístupů. Nastavuje ověřování pro připojované aplikace za pomoci podporovaných protokolů v daném prostředí. Zajišťuje federaci identit mezi jednotlivými prostředími. Nastavuje workflow pro lifecycle identit a přístupů. Spravuje nastavení autentizace a kde je to možné i autorizace. Navrhuje řešení problematiky autentizace a autorizace za použití autentizačních protokolů jako je SAML, OAuth, OpenID Connect, LDAP(s), Kerberos atd.
65	Metodik Kompetenčního centra SAP	Odpovídá za procesy KC SAP v rozsahu u daného zákazníka – Contract Management, Support Desk, Information Management, Coordination of Innovation Requests, Service Planning. Podílí se na návrhu a implementaci systému na platformě SAP. Podílí se na činnostech podpory provozu systémů na platformě SAP. Komunikuje vytvořené procesy s dalšími členy projektových týmů.
66	Metodik Monitoringu SAP	Odpovídá za procesy monitoringu SAP v rozsahu u daného zákazníka (SAP Solution Manager). Podílí se na návrhu a řešení systému monitoringu na platformě SAP. Podílí se na procesech podpory provozu systému na platformě SAP. Zajišťuje kontrolu nastavených

ID	Název Odborné role	Popis činností
		procesů monitoringu. Komunikuje vytvořené procesy s dalšími členy projektových týmů.
67	Metodik centrální správy uživatelů	Odpovídá za centrální správu uživatelů (CSU) v prostředí SAP v rozsahu u daného zákazníka. Podílí se na návrhu a řešení změn a návrhů procesů. Podílí se na procesech podpory provozu systémů na platformě SAP. Zajišťuje kontrolu nastavených procesů správa uživatelů. Komunikuje vytvořené procesy s dalšími členy projektových týmů.
68	Konzultant báze SAP	Provádí u zákazníka instalaci, údržbu, monitoring prostředí SAP, provádí instalace, upgrady a instalace podpůrných balíčků na ABAP a JAVA. Odpovídá za analýzu, návrh, plánování a provádění technických činností SAP v úzké spolupráci s projektovými týmy a týmy infrastruktury zákazníka. Odpovídá za konfigurace SAP Solution Manager pro monitorování. Provádí analytické činnosti z pohledu potřeb aplikace, business procesů a ICT prostředků. Provádí homogenní a heterogenní migrace databází a systémové kopie.
69	Konzultant SAP Identity Management	Odpovídá za konfiguraci Identity Management (SAP, NON-SAP), podporuje implementaci projektů a dokumentuje postupy. Odpovídá za správu identit a spolupracuje při změnách rozhraní. Odpovídá za správa životního cyklu uživatelů a management přístupu k informačním systémům. Spolupracuje na zvýšení bezpečnosti a zefektivnění zásadních procesů u zákazníků. Spolupracuje se specialistou bezpečnosti při řešení kybernetických bezpečnostních incidentů.
70	Konzultant SAP Enterprise Threat Detection	Podílí se na činnostech podpory produktů Enterprise Threat Detection SAP (ETD), zejména monitoring stavu, řešení problému při sběru a zpracování logu. Podílí se na kontrole provedených akcí, zpracování vzniklých upozornění, zpracování a vykazování založených pátrání. Kontroluje a identifikuje relevantních událostí v nerozpoznaných lozích, kontroluje detaily logů. Podílí se na nastavení výjimek pro generování upozornění. Odpovídá za optimalizaci a nastavení logiky zpracování událostí dle specifik prostředí.Odpovídá za konfiguraci systému SAP ETD, podporuje implementaci projektů a dokumentuje postupy. Odpovídá za správu ETD a spolupracuje při změnách zákazníka. Spolupracuje na zvýšení bezpečnosti a zefektivnění zásadních procesů u zákazníků. Spolupracuje se specialistou bezpečnosti při řešení kybernetických bezpečnostních incidentů.
71	Konzultant SAP Content Server	Podílí se na činnostech monitoringu a správy parametrů instalace SAP Content Server. Provádí správu a údržbu komponenty SAP Content Server. Spolupracuje na tvorbě na ukládání velkého množství elektronických dokumentů v jakémkoli formátu a s libovolným obsahem. Spolupracuje se specialistou bezpečnosti při řešení kybernetických bezpečnostních incidentů. Zodpovídá za tvorbu a aktuálnost dokumentace. Podílí se na kontrole procesu zálohování, archivace a obnovení. Kontroluje a identifikuje relevantních událostí v detailech logů. Zodpovídá za optimalizaci dle specifik prostředí.
72	Programátor ABAP	Provádí programátorskou činnost v oblasti SAP R/3. Zajišťuje vývoj nové funkcionality dle požadavků zákazníka. Odpovídá za údržbu existujících aplikací. Spolupracuje a účastní se jako člen týmu na roll out projektech a na implementaci SAP R/3. Spolupracuje při analýze a tvorbě nových řešení v oblasti SAP R/3 a kooperujících systémech.
73	Architekt /konzultant monitoringu senior	Provádí analýzu, návrh řešení architektury dle požadavků zákazníka. Provádí implementaci a administraci CA Spectrum, CA UIM, CA SOI, CA BIJS, CA APM, CA DX (dále jen "Produkty"). Testuje navrhovaná řešení a provádí úpravy nastavení. Spolupracuje na řešení uživatelských požadavků.
74	Administrátor monitoringu – infrastruktura senior	Provádí instalaci, údržbu všech produktů CA Broadcom dle doporučení výrobce. Provádí implementaci a administraci CA Spectrum, CA UIM, CA SOI, CA BIJS, CA APM, CA DX. Připravuje testovací scénáře,

ID	Název Odborné role	Popis činností
		testuje navrhovaná řešení a provádí úpravy nastavení. Podílí se na nastavování a aktualizaci bezpečnostních pravidel.
75	Analytik monitoringu	Provádí analýzu dle požadavků zákazníka. Provádí analytické činnosti z pohledu potřeb monitoringu, business procesů a ICT prostředků. Analyzuje výstupy monitoringu a připravuje scénáře pro řešení událostí a incidentů. Spolupracuje s bezpečnostním specialistou.
76	Specialista ElasticSearch – provoz senior	Provádí pokročilé činnosti v oblasti centrální správy logů. Provádí administraci Produktů ElasticSearch.
77	Specialista/konzultant ElasticSearch	Navrhuje a vyvíjí rozšíření produktů ElasticSearch. Navrhuje a implementuje SSO pro bezplatnou verzi ElasticSearch.Připravuje analýzu požadavků a přípravu konceptu řešení s využitím ElasticSearch. Instaluje a konfiguruje komponenty Elastic stacku – ElasticSearch, Logstash, Kibana atd. Plánuje a provádí upgrade platforem. Navrhuje design a implementaci řešení zahrnující konfiguraci datových agentů, přípravu konektorů pro sběr dat, konfiguraci datových pipeline, přípravu dashboardů, konfiguraci alertů a analytických jobů. Zajišťuje údržbu a rozvoj řešení s využitím ElasticSearch. Odpovídá za návrh a implementaci nových produktových komponent.
78	Konzultant SAP Process Integration Base Engine	Provádí údržbou / podporu SAP PI / SAP PO (funkční správa aplikací). Provádí konfiguraci výstrah a odstraňování problémů. Navrhuje a provádí migrace integračních scénářů ze SAP PI/PO (dual stack ABAP, JAVA). Navrhuje a provádí implementace workflow scénářů. Odpovídá za monitoring (PI komponenty, správy, performance) a za tvorbu a udržovaní dokumentace k nastavením a administraci SAP Process Integration Base Engine. Spolupracuje se specialistou bezpečnosti při řešení kybernetických bezpečnosntích incidentů.
79	Konzultant SAP Governance, Risk and Compliance	Provádí správu a údržbu SAP Governance, Risk and Compliance (GRC). Mapuje potenciální rizika zneužití oprávnění uživateli a automaticky upozorňuje na kombinaci kritických oprávnění. Spolupracuje na vytváření a změnách autorizačních rolí SAP. Spolupracuje na vytváření konceptů autorizace SAP. Provádí funkční testování implementovaných řešení SAP. Zodpovídá za tvorbu a udržovaní dokumentace k nastavením a administraci. Spolupracuje se specialistou bezpečnosti při řešení kybernetických bezpečnostních incidentů.
80	Konzultant SAP Single Sign-on	Podílí se na činnostech podpory produktu SAP Single Sign-on (SSO). Implementuje autorizační koncepty SAP se zaměřením na SoD. Vytváří procesní dokumenty/ koncepty v oblasti SAP Autorizace/IDM/Non SAP IDM. Spolupracuje při zavádění prostředí SAP IDM/non SAP IDM včetně integrace GRC/AC a migrace starších aplikací. Podílí se na optimalizaci a dalším rozvoji procesů / nástrojů pro správu uživatelů a oprávnění SAP. Zajišťuje podporu pro projekty ve všech fázích – od koncepce přes návrh až po uvedení do provozu. Koordinuje účast na podpoře za účelem rychlého řešení narušení v rámci podpory 1., 2. a 3. úrovně. Poskytuje součinnost při implementaci obchodních požadavků na straně systému (vytváření a údržba rolí, přizpůsobení v SAP/IDM/Non SAP IDM). Zodpovídá za tvorbu a udržovaní aktuální dokumentace k nastavením.
81	Konzultant SAP Code Vulnerability Analyzer	Podílí se na činnostech podpory produktů SAP Code Vulnerability Analyzer (CVA), zejména schvalování a zamítání výjimek založených vývojáři, nastavení běhu kontrol na objektech. Podílí se na kontrole výsledků běhů a oprav nahlášených problémů při provádění kontrol CVA. Navrhuje a doporučuje řešení oprav vzniklých hlášení při provádění kontrol CVA. Podílí se na vytváření bezpečnostních pravidel a politiky daného prostředí. Spolupracuje se specialistou bezpečnosti při řešení kybernetických bezpečnostních incidentů.

SPCSS
Státní pokladna
Centrum sdílených služeb

Ceník odborných rolí SPCSS

ID	Název Odborné role	Cena za 1 člověkoden			Cena za 1 člověkohodinu		
		v Kč bez DPH	DPH	v Kč včetně DPH	v Kč bez DPH	DPH	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 služeb 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 Microsoft technologií (MS)	13 000,00	2 730,00	15 730,00	1 625,00	341,25	1 966,25
11	Administrátor databáze (DB)	15 400,00	3 234,00	18 634,00	1 925,00	404,25	2 329,25
12	Administrátor správy a zálohování SAZ	14 400,00	3 024,00	17 424,00	1 800,00	378,00	2 178,00
13	Administrátor síťových technologií (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

Ceník dalších odborných rolí

ID	Název Odborné role	Cena za 1 člověkoden			Cena za 1 člověkohodinu		
		v Kč bez DPH	DPH	v Kč včetně DPH	v Kč bez DPH	DPH	v Kč včetně DPH
23 až 81	Další odborné role	Na základě požadavku Objednatele bude role zajištěna prostřednictvím veřejné zakázky. Jednotlivé ceny budou uvedeny v konkrétní Nabídce a následné Objednávce, včetně případného harmonogramu plnění.					

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 3 – Vzor nabídky

Identifikační údaje Objednatele	**Identifikační údaje Poskytovatele**
Česká republika – Ministerstvo zahraničních věcí se sídlem: Loretánské nám. 101/5, 118 00 Praha 1 za niž jedná: [DOPLNÍ MZV] IČO: 45769851 DIČ: CZ45769851 Bank. spojení: [DOPLNÍ MZV] číslo účtu: [DOPLNÍ MZV] ID DS: e4xaaxh	**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: [redacted] IČO: 036 30 919 DIČ: CZ03630919 Bank. spojení: [redacted] číslo účtu: [redacted] 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 Služby	[bude doplněno v případě Nabídky na Službu dle čl. II odst. 2.4 pododst. 2.4.1
Celková cena za nabízený počet člověkodnů	[bude doplněno v případě Nabídky na Službu dle čl. II odst. 2.4 poddost. 2.4.2
Celková cena za nabízené Ostatní činnosti	[bude doplněno v případě Nabídky na Službu dle čl. II odst. 2.4 poddost. 2.4.3
Podrobná specifikace požadované Služby včetně rozsahu	
Popis řešení (vč. uvedení případných poddodavatelů a části Plnění, 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]
Požadavky na součinnost třetích stran	[bude doplněno]

Schvalovací doložka

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

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 4 – Objednávka

Příloha č. 4.1 – Objednávka Služby– VZOR

OBJEDNÁVKA

Služby

číslo **[BUDE DOPLNĚNO]**
č. j. **[BUDE DOPLNĚNO]**
vystavena dne **[BUDE DOPLNĚNO]**

Název a číslo projektu SF EU			
[BUDE DOPLNĚNO OBJEDNATELEM]			
Objednatel		**Poskytovatel**	
Název	**Česká republika – Ministerstvo zahraničních věcí**	Název	**Státní pokladna Centrum sdílených služeb, s. p.**
Sídlo	Loretánské nám. 101/5 118 00 Praha 1	Sídlo	Na Vápence 915/14 Žižkov, 130 00 Praha 3
IČO	45769851	IČO	036 30 919
DIČ	CZ45769851	DIČ	CZ03630919
Vystavil	[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 Služby:

P. č.	Specifikace Předmětu plnění	Měsíční cena v Kč bez DPH	Měsíční cena v Kč včetně DPH
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]
Celkem za celou dobu plnění Služby		[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]

Podrobná specifikace Služby	[BUDE DOPLNĚNO S ODKAZEM NA PŘÍPADNOU PŘÍLOHU TÉTO OBJEDNÁVKY]
Termín plnění (Harmonogram)	[BUDE DOPLNĚNO]
Místo plnění	[BUDE DOPLNĚNO]
Podrobná specifikace bezpečnostních podmínek	[BUDE DOPLNĚNO, JE-LI TO NUTNÉ]
Stanovení smluvních pokut	[BUDE DOPLNĚNO]

Realizační tým	[BUDE DOPLNĚNO S ODKAZEM NA PŘÍPADNOU PŘÍLOHU TÉTO OBJEDNÁVKY]		
Kvalitativní a technické parametry	[BUDE DOPLNĚNO S ODKAZEM NA PŘÍPADNOU PŘÍLOHU TÉTO OBJEDNÁVKY]		
Požadavky na součinnost třetích stran	[BUDE DOPLNĚNO, JE-LI TO NUTNÉ]		
Poznámka	[BUDE DOPLNĚNO]		
Vystavil za Objednatele		**Akceptoval 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.			

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 4 – Objednávka

Příloha č. 4.2 – Objednávka Konzultace – VZOR

OBJEDNÁVKA

Konzultace

číslo	**[BUDE DOPLNĚNO]**
č. j.	**[BUDE DOPLNĚNO]**
vystavena dne	**[BUDE DOPLNĚNO]**

Název a číslo projektu SF EU			
[BUDE DOPLNĚNO OBJEDNATELEM]			
Objednatel		**Poskytovatel**	
Název	**Česká republika – Ministerstvo zahraničních věcí**	Název	**Státní pokladna Centrum sdílených služeb, s. p.**
Sídlo	Loretánské nám. 101/5 118 00 Praha 1	Sídlo	Na Vápence 915/14 Žižkov, 130 00 Praha 3
IČO	45769851	IČO	036 30 919
DIČ	CZ45769851	DIČ	CZ03630919
Vystavil	[BUDE DOPLNĚNO]		
Smlouva	**Rámcová smlouva o poskytování služeb datového centra** (dále jen „**Smlouva**“)		
Kontaktní os.	[BUDE DOPLNĚNO]	**Kontaktní os.**	[BUDE DOPLNĚNO]
Telefon	[BUDE DOPLNĚNO]	Telefon	[BUDE DOPLNĚNO]
E-mail	[BUDE DOPLNĚNO]	E-mail	[BUDE DOPLNĚNO]

Objednatel objednává od Poskytovatele následující Konzultace

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		[BUDE DOPLNĚNO]	ČH	---	[BUDE DOPLNĚNO]
Celkem					[BUDE DOPLNĚNO]

Specifikace Konzultací	[BUDE DOPLNĚNO]
Termín plnění (Harmonogram)	[BUDE DOPLNĚNO]
Místo plnění	[BUDE DOPLNĚNO]
Podrobná specifikace bezpečnostních podmínek	[BUDE DOPLNĚNO, JE-LI TO NUTNÉ]
Stanovení smluvních pokut	[BUDE DOPLNĚNO]
Realizační tým	[BUDE DOPLNĚNO S ODKAZEM NA PŘÍPADNOU PŘÍLOHU TÉTO OBJEDNÁVKY]

Poznámka	[BUDE DOPLNĚNO]		
Vystavil za Objednatele		**Akceptoval za Poskytovatele**	
Jméno, příjmení	[BUDE DOPLNĚNO]	**Jméno, příjmení**	[BUDE DOPLNĚNO]
Datum a podpis		**Datum a podpis**	

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 4 – Objednávka

Příloha č. 4.3 – Objednávka Ostatní činnosti – VZOR

OBJEDNÁVKA

Ostatní činnosti

číslo	**[BUDE DOPLNĚNO]**
č. j.	**[BUDE DOPLNĚNO]**
vystavena dne	**[BUDE DOPLNĚNO]**

Název a číslo projektu SF EU	
[BUDE DOPLNĚNO OBJEDNATELEM]	

Objednatel		**Poskytovatel**	
Název	**Česká republika – Ministerstvo zahraničních věcí**	Název	**Státní pokladna Centrum sdílených služeb, s. p.**
Sídlo	Loretánské nám. 101/5 118 00 Praha 1	Sídlo	Na Vápence 915/14 Žižkov, 130 00 Praha 3
IČO	45769851	IČO	036 30 919
DIČ	CZ45769851	DIČ	CZ03630919
Vystavil	[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.	Specifikace Předmětu plnění	Cena za jednotku v Kč bez DPH	Cena celkem v Kč bez DPH
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	0,00 Kč
Celkem			[BUDE DOPLNĚNO]

Podrobná specifikace Ostatních činností	[BUDE DOPLNĚNO S ODKAZEM NA PŘÍPADNOU PŘÍLOHU TÉTO OBJEDNÁVKY]
Termín plnění (Harmonogram)	[BUDE DOPLNĚNO]
Místo plnění	[BUDE DOPLNĚNO]
Podrobná specifikace bezpečnostních podmínek	[BUDE DOPLNĚNO, JE-LI TO NUTNÉ]
Stanovení smluvních pokut	[BUDE DOPLNĚNO]
Realizační tým	[BUDE DOPLNĚNO S ODKAZEM NA PŘÍPADNOU PŘÍLOHU TÉTO OBJEDNÁVKY]
Akceptační kritéria	[BUDE DOPLNĚNO S ODKAZEM NA PŘÍPADNOU PŘÍLOHU TÉTO OBJEDNÁVKY]

Kvalitativní a technické parametry	[BUDE DOPLNĚNO S ODKAZEM NA PŘÍPADNOU PŘÍLOHU TÉTO OBJEDNÁVKY]		
Poznámka	[BUDE DOPLNĚNO]		
Vystavil za Objednatele		**Akceptoval 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.			

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 5 – Záznam o poskytnutí Služeb – VZOR

Záznam o poskytnutí Služeb – VZOR

dle Rámcové smlouvy o poskytování služeb datového centra
(evid. u Poskytovatele pod č. SML2024139 a u Objednatele pod č. [DOPLNÍ MZV])

Vykazované období:	od	do

Obě Smluvní strany potvrzují, že v uvedeném období byly v souladu s výše uvedenou Rámcovou smlouvou *(toto ustanovení se nijak nedotýká práv a povinností dle čl. 5.2 – 5.4 Rámcové smlouvy)* poskytnuty níže specifikované Služby v účtovaném množství:

Služba – Objednávka č.	**Cena za období v Kč bez DPH**	**DPH v Kč**	**Cena za období v Kč včetně DPH**
Celkem			

Detailní přehled poskytnutých Služeb, hodnocení kvality Služeb a kontrola plnění dle konkrétní Objednávky bude uvedeno v měsíční Zprávě o úrovni a rozsahu poskytovaných Služeb.

Za Objednatele	**Za Poskytovatele**
Datum:	Datum:
Jméno, příjmení Oprávněné osoby Objednatele:	Jméno, příjmení Oprávněné osoby Poskytovatele:
Podpis:	Podpis:

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 6 – Vzor Zprávy

Státní pokladna Centrum sdílených služeb, s. p.

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

ZPRÁVA – VZOR

o úrovni a rozsahu poskytovaných Služeb v období

[DOPLNÍ MZV] – [DOPLNÍ MZV]

dle Rámcové smlouvy o poskytování služeb datového centra
(evid. u Poskytovatele pod č. SML2024139 a u Objednatele pod č. [DOPLNÍ MZV])

1. **OBDOBÍ A REŽIM POSKYTOVÁNÍ SLUŽEB**
2. **ROZSAH POSKYTOVANÝCH SLUŽEB**
3. **ŘEŠENÍ ZÁVAD**
4. **SERVISNÍ ZÁSAHY a PROVOZNÍ ZMĚNY**
5. **DOSTUPNOST SLUŽEB**
6. **Celkový PŘEHLED OMEZENÍ SLUŽEB**
7. **PROBLÉMY A RIZIKA**
8. **ZPRÁVA O STAVU BEZPEČNOSTI**
9. **SMLUVNÍ POKUTY**
10. **PŘÍLOHY**
11. **PODPISOVÁ DOLOŽKA**

Zpráva Poskytovatele:

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

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 7 – Odpovědné osoby

Odpovědné osoby Poskytovatele:

[redacted]

Odpovědné osoby Objednatele:

[redacted]

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 8 – Vzor Výkazu

VÝKAZ KONZULTACE					
Předmět	[BUDE DOPLNĚNO]				
Smlouva (dále jen „**Smlouva**“)	[BUDE DOPLNĚNO]				
Objednatel (dále jen „**Objednatel**“)	[BUDE DOPLNĚNO – NÁZEV, IČO]				
Poskytovatel (dále jen „**Poskytovatel**“)	[BUDE DOPLNĚNO – NÁZEV, IČO]				
Vykazované období	od DD.MM.RRRR do DD.MM.RRRR				
Vypracoval	[BUDE DOPLNĚNO]		**Datum**	[BUDE DOPLNĚNO]	
Výkaz					
Název	**Role**	**Množství**	**MJ**	**Cena za jednotku v Kč bez DPH**	**Cena celkem v Kč bez DPH**
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]
Připomínky Objednatele					
Připomínky k rozsahu a kvalitě poskytované služby					
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

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 9 – Vzor Akceptačního protokolu

AKCEPTAČNÍ PROTOKOL

Předmět	[BUDE DOPLNĚNO]		
Smlouva (dále jen „**Smlouva**")	Rámcová smlouva o poskytování služeb datového centra		
Objednatel (dále jen „**Objednatel**")	[BUDE DOPLNĚNO – NÁZEV, IČO]		
Poskytovatel (dále jen „**Poskytovatel**")	[BUDE DOPLNĚNO – NÁZEV, IČO]		
Vypracoval	[BUDE DOPLNĚNO]	**Datum**	[BUDE DOPLNĚNO]

Předmět akceptace
Hodnocení, kontrola plnění a akceptace poskytovaných Ostatních činností
Připomínky Objednatele
Připomínky k rozsahu a kvalitě poskytovaných Ostatních činností
Závěry akceptace

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

Akceptace

Název	Popis	Termín dodání	Cena v Kč bez DPH
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]
[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]	[BUDE DOPLNĚNO]

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	Popis Ostatních činností
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

Rámcová smlouva o poskytování služeb datového centra

Příloha č. 10: Ceník Služeb kybernetické bezpečnosti

	Popis rozsahu Služby	v Kč bez DPH	DPH	v Kč včetně DPH
Služba KL01	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	1 102,00 Kč	231,42 Kč	1 333,42 Kč
	501 - 1 000	500,73 Kč	105,15 Kč	605,88 Kč
	1 001 - 2 000	345,90 Kč	72,64 Kč	418,54 Kč
	2 001 - 5 000	250,97 Kč	52,70 Kč	303,67 Kč
	5 001 - 10 000	211,18 Kč	44,35 Kč	255,53 Kč
	10 001 - 15 000	196,99 Kč	41,37 Kč	238,36 Kč
	15 001 - 20 000	191,72 Kč	40,26 Kč	231,98 Kč
	20 001 - 25 000	188,16 Kč	39,51 Kč	227,67 Kč
	25 001 - 30 000	186,41 Kč	39,15 Kč	225,56 Kč
	30 001 - 40 000	183,92 Kč	38,62 Kč	222,54 Kč
Doplňkové služby KL01	Rozsah Služby	v Kč bez DPH za měsíc	DPH	v Kč včetně DPH za měsíc
Bezpečnostní monitoring databází	1 ks/databáze	27 534,01 Kč	5 782,14 Kč	33 316,15 Kč
Virtuální kolektor - Bezpečnostní monitoring databází	1 ks/kolektor	11 095,13 Kč	2 329,98 Kč	13 425,11 Kč
Virtuální agregátor - Bezpečnostní monitoring databází	1 ks/agregátor	11 095,13 Kč	2 329,98 Kč	13 425,11 Kč
Virtualizace DB - Virtuální kolektor pro Bezpečnostní monitoring databází	virtualizace pro 1 kolektor (32 BB, 600 GB)	13 212,19 Kč	2 774,56 Kč	15 986,75 Kč
Virtualizace DB - Virtuální agregátor pro Bezpečnostní monitoring databází	virtualizace pro 1 agregátor (32 BB, 1 536 GB)	16 010,93 Kč	3 362,30 Kč	19 373,23 Kč
Virtuální kolektor - Bezpečnostní monitoring	1 ks/kolektor	2 034,34 Kč	427,21 Kč	2 461,55 Kč
Virtuální procesor - Bezpečnostní monitoring	1 ks/procesor	2 034,34 Kč	427,21 Kč	2 461,55 Kč
Virtualizace BM - Virtuální kolektor pro Bezpečnostní monitoring	virtualizace pro 1 kolektor (64 BB, 512 GB)	10 808,71 Kč	2 269,83 Kč	13 078,54 Kč
Virtualizace BM - Virtuální procesor pro Bezpečnostní monitoring	virtualizace pro 1 procesor (112 BB, 1 024 GB)	19 297,89 Kč	4 052,56 Kč	23 350,45 Kč
Úložný prostor	256 GB	765,49 Kč	160,75 Kč	926,24 Kč
Služba KL02	Rozsah Služby	v Kč bez DPH	DPH	v Kč včetně DPH
Analýza rizik	dle KL02	Bude oceněno v souladu s Přílohou č. 2 Smlouvy a následně uvedeno v konkrétní Nabídce a navazující Objednávce		
Služba KL03	Rozsah Služby	v Kč bez DPH	DPH	v Kč včetně DPH
Analýza rizik předmětu veřejné zakázky	dle KL03	Bude oceněno v souladu s Přílohou č. 2 Smlouvy a následně uvedeno v konkrétní Nabídce a navazující Objednávce		

Služba KL04	Rozsah Služby	v Kč bez DPH	DPH	v Kč včetně DPH
Penetrační testy	dle KL04	Bude oceněno v souladu s Přílohou č. 2 Smlouvy (případně na základě veřejné zakázky) a následně uvedeno v konkrétní Nabídce a navazující Objednávce		
Služba KL05	Rozsah Služby	v Kč bez DPH za 1 člověkoden	DPH	v Kč včetně DPH za 1 člověkoden
Konzultace v oblasti informační a kybernetické bezpečnosti	dle KL05	Cena dle rozsahu a akceptace - dle sazby za 1 člověkoden uvedené v Příloze č. 2 Smlouvy		
Služba KL06	Rozsah Služby	v Kč bez DPH za měsíc	DPH	v Kč včetně DPH za měsíc
Vulnerability management	1 CI	343,64 Kč	72,16 Kč	415,80 Kč
Vulnerability management - engine	1 ks engine	12 201,64 Kč	2 562,34 Kč	14 763,98 Kč
Virtualizace pro nasazení 1 engine	virtualizace pro 1 ks engine (4 BB, 100 GB, správa)	4 841,83 Kč	1 016,78 Kč	5 858,61 Kč
Úložný prostor	256 GB	765,49 Kč	160,75 Kč	926,24 Kč
Služba KL07	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	243 043,21 Kč	51 039,07 Kč	294 082,28 Kč
	SŘBI do správy 50 dokumentů	270 918,35 Kč	56 892,85 Kč	327 811,20 Kč
	SŘBI do správy 75 dokumentů	298 793,49 Kč	62 746,63 Kč	361 540,12 Kč
	SŘBI do správy 100 dokumentů	391 710,61 Kč	82 259,23 Kč	473 969,84 Kč
	SŘBI do správy 150 dokumentů	484 627,74 Kč	101 771,83 Kč	586 399,57 Kč
	SŘBI do správy 200 dokumentů	540 378,01 Kč	113 479,38 Kč	653 857,39 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. 2 Smlouvy		

SPCSS
Státní pokladna
Centrum sdílených služeb

Služba KL08	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 a Session Recording (jednotka - počet souběžných uživatelů)	1 - 50	4 123,77 Kč	865,99 Kč	4 989,76 Kč
	51 - 100	2 626,47 Kč	551,56 Kč	3 178,03 Kč
	101 - 150	2 327,01 Kč	488,67 Kč	2 815,68 Kč
	151 - 200	2 198,67 Kč	461,72 Kč	2 660,39 Kč
	201 - 250	2 127,37 Kč	446,75 Kč	2 574,12 Kč
	251 - 300	2 082,00 Kč	437,22 Kč	2 519,22 Kč
Doplňkové Služby KL08	**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	12 624,89 Kč	2 651,23 Kč	15 276,12 Kč
	balíček 50	22 830,84 Kč	4 794,48 Kč	27 625,32 Kč
	balíček 75	31 277,56 Kč	6 568,29 Kč	37 845,85 Kč
	balíček 100	38 404,84 Kč	8 065,02 Kč	46 469,86 Kč
	balíček 125	44 517,19 Kč	9 348,61 Kč	53 865,80 Kč
	balíček 150	49 832,09 Kč	10 464,74 Kč	60 296,83 Kč
	balíček 175	54 509,03 Kč	11 446,90 Kč	65 955,93 Kč
	balíček 200	58 667,62 Kč	12 320,20 Kč	70 987,82 Kč
	balíček 225	62 399,34 Kč	13 103,86 Kč	75 503,20 Kč
	balíček 250	65 775,34 Kč	13 812,82 Kč	79 588,16 Kč
	balíček 275	68 851,76 Kč	14 458,87 Kč	83 310,63 Kč
	balíček 300	71 673,57 Kč	15 051,45 Kč	86 725,02 Kč