RÁMCOVÁ SMLOUVA O POSKYTOVÁNÍ SLUŽEB V OBLASTI INFORMAČNÍ A KYBERNETICKÉ BEZPEČNOSTI

evidovaná u Objednatele pod č. 24/7700/0034
evidovaná u Poskytovatele pod č. SML2024019, č. j. SPCSS-01474/2024
(dále jen „**Smlouva**")

Smluvní strany:
Česká republika – Generální finanční ředitelství
se sídlem: Lazarská 15/7, 117 22 Praha 1
za niž jedná: [redacted] generální ředitelka
IČO: 72080043
DIČ: CZ72080043
bankovní spojení: [redacted]
č. účtu:
ID DS: p9iwj4f

(dále jen „**Objednatel**" nebo „**GFŘ**")

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] 1. zástupcem generálního ředitele
IČO: 036 30 919
DIČ: CZ03630919
bankovní spojení: ČNB
číslo účtu: [redacted]
ID DS:

(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 „**ZZVZ**")

I. ÚVODNÍ USTANOVENÍ

1.1 Objednatel prohlašuje, že:

1.1.1 je orgánem Finanční správy České republiky, jakožto soustavy správních orgánů pro výkon správy daní, jehož působnost a činnosti jsou stanoveny zákonem č. 456/2011 Sb., o Finanční správě České republiky, ve znění pozdějších předpisů, a

1.1.2 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 rovněž 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 „**ZoKB**" nebo „**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 „**VoKB**" nebo „**Vyhláška o kybernetické bezpečnosti**"), a zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále jen „**ZoZOU**").

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

1.4 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 informační a kybernetické bezpečnosti. 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 informační a 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 následující služby:

2.4.1 Bezpečnostní monitoring – Služba je poskytována v nepřetržitém režimu 24x7 (tj. 24 hodin denně, 7 dní v týdnu) a zahrnuje sběr informací, jejich třídění, korelaci, kategorizaci, analýzu a archivaci. Použité technologie a nástroje umožňují detekci známých bezpečnostních útoků, podezřelého chování a anomálií. Součástí je proces zvládání kybernetických bezpečnostních incidentů (to vše dále jen **„Bezpečnostní monitoring**"). Přičemž podrobná specifikace Bezpečnostního monitoringu je uvedena v Příloze č. 1 Smlouvy.

2.4.2 Log management – Služba zajišťuje funkcionalitu log managementu a zpracování logů pro vizualizaci a sledování logů vybraných zařízení, operačních systémů a aplikací. Výsledné řešení zajistí dodržovaní požadavku Zákona o kybernetické bezpečnosti, a vyhlášky o kybernetické bezpečnosti, na centrální ukládání a archivaci logů GFŘ (to vše dále jen „**Log management**"). Přičemž podrobná specifikace Log managementu je uvedena v Příloze č. 2 Smlouvy.

2.4.3 Správa privilegovaných účtů – Služba obsahuje správu přístupu k privilegovaným účtům a monitoring veškeré aktivity těchto účtů (to vše dále jen „**Správa privilegovaných účtů**"). Přičemž podrobná specifikace Správy privilegovaných účtů je uvedena v Příloze č. 3 Smlouvy.

2.4.4 Kompetenční centrum kybernetické bezpečnosti – Služba zahrnuje podporu činností vyplývajících pro povinné osoby Objednatele z právních předpisů, zejména Zákon o kybernetické bezpečnosti, resp. Vyhláška o kybernetické bezpečnosti, a skládá se z následujících dvou částí:

2.4.4.1 Administrace dokumentace v Nástroji pro podporu řízení SŘBI – Služba zajišťuje správu a evidenci klíčové agendy kybernetické bezpečnosti v Nástroji pro podporu řízení SŘBI tak, aby byly podpořeny procesy a centralizovány informace o povinných činnostech v souladu s požadavky Zákona o kybernetické bepečnosti, resp. Vyhlášky o kybernetické bezpečnosti (to vše dále jen „**Administrace SŘBI**");

2.4.4.2 Metodická podpora v oblasti SŘBI – Služba obsahuje metodickou, procesní a dokumentační podporu v oblasti informační a kybernetické bezpečnosti v souladu s požadavky Zákona o kybernetické bepečnosti, resp. Vyhlášky o kybernetické bezpečnosti (to vše dále jen „**Metodická podpora**");

(Administrace SŘBI a Metodická podpora dále také společně jen „**KCKB**"), přičemž podrobná specifikace KCKB je uvedena v Příloze č. 4 Smlouvy;

2.4.5 Konzultace v oblasti informační a kybernetické bezpečnosti – Služba obsahuje 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 a poskytnutí rozvojových činností v oblasti syslog serverů, a to vše formou poskytnutí činností rolí (dále jen „**Konzultace**"). Přičemž podrobná specifikace Konzultací je uvedena v Příloze č. 5 Smlouvy;

2.4.6 Vulnerability management – Služba je ucelené řešení pro správu zranitelností ICT prostředí Objednatele (dále jen „**Vulnerability management**"). Přičemž podrobná specifikace Vulnerability managementu je uvedena v Příloze č. 6 Smlouvy;

2.4.7 Správa syslog serverů – Služba zahrnuje správu operačního systému serverů dedikovaných pro provoz syslog serverů a na nich provozovaných Syslog NG serverů (dále jen „**Správa syslog serverů**"), přičemž podrobná specifikace Správy syslog serverů je uvedena v Příloze č. 7 Smlouvy;

(to vše dále jednotlivě také jen „**Služba"** nebo společně jen „**Služby**").

Služby uvedené v odst. 2.4.1, 2.4.2, 2.4.3, 2.4.6 a 2.4.7 v souhrnu představují ucelené řešení služeb „Security Operations Center", kdy v rámci podrobné specifikace těchto Služeb uvedených v jednotlivých přílohách Smlouvy, je stanoven rozsah pokrytí uložených povinností dle VoKB.

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 Přílohách č. 1 až č. 4 Smlouvy, Příloze č. 6 a Příloze č. 7 Smlouvy.

2.6 Poskytovatel je povinen poskytnout Objednateli data, která Poskytovatel shromáždil v průběhu poskytování Služeb a na základě kterých vytvořil výstupy v rámci Služeb. 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. Poskytovatel předá data Objednateli v termínech a způsobem stanoveným v příslušné Objednávce v souladu s platnými a účinnými právními předpisy.

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

2.8 Smluvní strany berou na vědomí a souhlasí s tím, že v rámci poskytování Služeb je zřízena řídicí struktura poskytování Služeb, jejíž činnosti a způsob řízení Služeb jsou definovány v Příloze č. 8 Smlouvy. V rámci řídicí struktury provozu Služeb se Smluvní strany zavazují zřídit následující orgány (dále jen „**Řídicí orgány**"):

2.8.1 Řídicí komisi (dále jen „**ŘKO**"), která je orgánem pro rozhodování o zásadních otázkách ovlivňujících poskytování Služeb. ŘKO je složena ze zástupců Objednatele a Poskytovatele. Podrobná specifikace činnosti ŘKO je uvedena v Příloze č. 8 Smlouvy.

2.8.2 Tým přípravy a poskytování Služeb (dále jen „**TPP**"), který je složen ze zástupců Poskytovatele a Objednatele, a příp. jejich poddodavatele. Podrobná specifikace činnosti TPP je uvedena v Příloze č. 8 Smlouvy.

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

2.10 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, která 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.

2.11 Poskytovatel prohlašuje, že disponuje veškerými potřebnými oprávněními pro poskytování Služeb.

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

2.13 Smluvní strany berou na vědomí, že v rámci plnění Smlouvy a jednotlivých Objednávek může docházet ke sběru dat ve smyslu VoKB, přičemž se jedná o data, která jsou ve vlastnictví Objednatele, a se kterými bude Poskytovatel nakládat pouze dle pokynů Objednatele.

2.14 Poskytovatel je povinen poskytnout Objednateli veškerá 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 příslušné Služby 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**").

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. Veškerá komunikace vedoucí k uzavření Objednávky bude probíhat prostřednictvím e-mailové korespondence Oprávněných osob Smluvních stran. 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 až Příloze č. 7 Smlouvy. Aniž by bylo dotčeno předcházející znění, Smluvní strany uvádějí, že realizace Metodické podpory a 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.

4.2 Realizace Služeb bude probíhat na základě jednotlivých Objednávek uzavíraných vždy zvlášť pro daný typ Služeb, na základě písemné výzvy Objednatele k poskytnutí dané Služby, 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;

4.2.3 specifikaci požadované Služby a včetně specifikace jejího rozsahu;

4.2.4 v případě Konzultací a Metodické podpory rovněž popis jednotlivých poptávaných rolí a případně jejich požadované certifikace;

4.2.5 případný požadavek na vypracování postupu plnění Exit plánu dle definice ve Smlouvě;

4.2.6 podpis Oprávněné osoby Objednatele.

4.3 Poskytovatel může bez zbytečného odkladu nejpozději však do 3 pracovních dnů ode dne doručení Výzvy požádat o doplnění či upřesnění specifikace požadované Služby 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 doručení řádně upravené/doplněné nové Výzvy Objednatelem.

4.4 Na základě Výzvy dle odst. 4.2 tohoto článku Smlouvy, a ve lhůtě maximálně 10 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. 9 (dále jen „**Nabídka**“).

4.5 Nabídka musí mj. obsahovat:

4.5.1 přesnou specifikaci a rozsah Služby, která má být na základě příslušné Objednávky poskytována dle Přílohy č. 1 až Přílohy č. 7 Smlouvy (v případě Konzultací a Metodické podpory rovněž počet nabízených člověkodnů);

4.5.2 nabídkovou cenu stanovenou v souladu se Smlouvou, tj. v souladu s Přílohou č. 13 Smlouvy a dle principu stanovení ceny uvedeného vždy pro danou Službu v Příloze č. 1 až Příloze č. 7 Smlouvy, a to vždy v rozpadu na jednotlivé požadavky dané Služby;

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

4.5.4 harmonogram plnění Služby, pokud bude relevantní v rámci dané Služby;

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

4.5.6 SLA pro předmětnou Službu, v případě, že se bude jednat o SLA požadovaná odlišně od SLA stanovených v Příloze č. 1 až Příloze č. 4, Příloze č. 6 a Příloze č. 7 Smlouvy a případně rovněž smluvní pokuty za nedodržení SLA dané Služby, pokud budou stanovena odlišně od SLA stanovených v Příloze č. 1 až Příloze č. 4 Smlouvy, Příloze č. 6 a Příloze č. 7 Smlouvy;

4.5.7 členy realizačního týmu Poskytovatele vč. doložení jejich certifikace, bude-li vyžadována, pokud bude jejich uvedení relevantní v rámci dané Služby;

4.5.8 požadovaný termín zahájení a ukončení poskytování Služby;

4.5.9 harmonogram a návrh postupu plnění Exit plánu, v případě, že byl požadován;

4.5.10 podpis Oprávněné osoby Poskytovatele.

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. 10 (dále jen „**Objednávka**"), zpracovaný dle akceptované Nabídky a dle podmínek této Smlouvy, a to nejpozději do 10 dnů ode dne doručení akceptace Nabídky. Návrh Objednávky Objednatel předloží k vyjádření všem dotčeným orgánům a na základě případně obdržených vyjádření 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 Objednatelem o těchto podmínkách jednat. Obě strany jsou při těchto jednáních povinny postupovat tak, aby došlo co nejdříve k uzavření Objednávky. Do doby uzavření Objednávky mají Smluvní strany právo na zrušení Objednávky ze závažných důvodů.

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 kterou Službu dle této Smlouvy se jedná a přesnou specifikaci a rozsah Služby, která má být na základě příslušné Objednávky poskytována dle Přílohy č. 1 až Přílohy č. 7 Smlouvy (v případě Konzultací a Metodické podpory rovněž uvedení počtu objednaných člověkodnů);

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

4.8.6 Místo plnění;

4.8.7 cenu stanovenou v souladu se Smlouvou, tj. v souladu s Přílohou č. 13 Smlouvy a dle principu stanovení ceny uvedeného vždy pro danou Službu v Příloze č. 1 až Příloze č. 7 Smlouvy, a to vždy v rozpadu na jednotlivé požadavky dané Služby;

4.8.8 vymezení součinnosti Smluvních stran;

4.8.9 členy realizačního týmu Poskytovatele dle Nabídky, pokud bude jejich uvedení relevantní v rámci dané Služby;

4.8.10 dobu trvání a ukončení poskytování Služby;

4.8.11 harmonogram realizace, pokud bude relevantní v rámci dané Služby;

4.8.12 SLA pro předmětnou Službu, v případě, že bude jednat o SLA požadovaná odlišně od SLA stanovených v Příloze č. 1 až Příloze č. 4 Smlouvy, Příloze č. 6 a Příloze č. 7 Smlouvy a případně rovněž smluvní pokuty za nedodržení SLA dané Služby, pokud budou stanovena odlišně od SLA stanovených v Příloze č. 1 až Příloze č. 4 Smlouvy, Příloze č. 6 a Příloze č. 7 Smlouvy;

4.8.13 akceptační kritéria, pokud budou relevantní v rámci dané Služby, přičemž nesmí být v rozporu v procesem akceptace Služeb dle čl. V Smlouvy;

4.8.14 podpisy Odpovědných osob ve věcech smluvních obou Smluvních stran;

4.8.15 harmonogram a obsah postupu plnění Exit plánu, v případě, že byl požadován;

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

4.9 Pro vyloučení pochybností Smluvní strany uvádějí, že k ujednání smluvních pokut odlišně od smluvních pokut stanovených v čl. XIII Smlouvy může dojít pouze v rámci odst. 13.5 a odst. 13.6. Smlouvy, tj. pouze v případě, že dojde ke sjednání SLA odlišných od SLA stanovených v Příloze č. 1 až Příloze č. 4, Příloze č. 6 a Příloze č. 7 Smlouvy. Jiná ujednání o smluvních pokutách nad rámec Smlouvy jsou neplatná.

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

4.11 Při plnění Objednávek je Poskytovatel povinen postupovat v souladu s touto Smlouvou a s danou Objednávkou. Na základě uzavřené Objednávky se Poskytovatel zavazuje poskytnout požadované Služby.

4.12 Poskytovatel se zavazuje v rámci realizace Konzultací a Metodické podpory dle každé předmětné Objednávky vést výkaz Konzultací nebo Metodické podpory (dle dané Objednávky), v rámci kterého prokazuje skutečně vynaložený čas na Konzultace nebo Metodickou podporu s přesností na celé člověkohodiny, a to vždy s uvedením konkrétních vykonaných činností v rámci Konzultací nebo Metodické podpory (dále jen „**Výkaz**").

V. AKCEPTACE SLUŽEB

5.1 Potvrzení o poskytnutí Služeb dle čl. II odst. 2.4 pododst. 2.4.1 až pododst. 2.4.4 Smlouvy (pro vyloučení pochybností Smluvní strany uvádějí, že v případě Služby dle pododst. 2.4.4 se odst. 5.1 až 5.3 tohoto článku Smlouvy vztahuje pouze na Administraci SŘBI), pododst. 2.4.6 a pododst. 2.4.7 Smlouvy v rámci všech účinných Objednávek uzavřených na základě této Smlouvy, bude realizováno formou podpisu Oprávněných osob Smluvních stran na společném záznamu o poskytnutí uvedených Služeb, jehož vzor je součástí Přílohy č. 11 Smlouvy (dále jen „**Záznam**"), a to následovně:

5.1.1 Poskytovatel se zavazuje vystavit Záznam za příslušný kalendářní měsíc do 5 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 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:

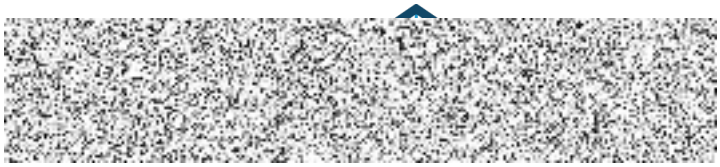
5.2.1 Objednatel provádí kontrolu plnění předmětných Služeb na základě zprávy o úrovni a rozsahu poskytovaných Služeb v rámci všech účinných Objednávek v příslušném období (dále jen „**Zpráva**"), přičemž vzor Zprávy je součástí Přílohy č. 12 Smlouvy. Kontrola plnění předmětných Služeb může být ze strany Objednatele prováděna též v Místě plnění během obvyklé pracovní doby, a to po předchozí domluvě s Poskytovatelem.

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

5.2.3 Objednatel se zavazuje ve lhůtě 5 pracovních dnů ode dne předložení Zprávy zpracovat ke Zprávě písemné stanovisko, kterým Zprávu akceptuje nebo neakceptuje.

5.2.4 V případě, že nebude Zpráva Objednatelem ve lhůtě dle pododst. 5.2.3 akceptována, zavazují se Smluvní strany zahájit jednání o sporných bodech, a to do 5 pracovních dnů ode dne doručení stanoviska dle předchozí věty Poskytovateli na jednání Oprávněných osob Smluvních stran, přičemž 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 v příslušném období 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 a/nebo Metodické podpory bude probíhat vždy za každý uplynulý kalendářní měsíc účinnosti předmětné Objednávky, v kterém byly Konzultace a/nebo Metodická podpora poskytovány.

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

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

5.7 Oprávněná osoba Objednatele se zavazuje Výkaz ve lhůtě 5 pracovních dnů ode dne doručení Výkazu svým podpisem schválit, případně do něj uvést výhrady. Poskytovatel se zavazuje vypořádat případné výhrady nejpozději do 5 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 Pro vyloučení pochybností Smluvní strany uvádějí, že v případě, že součástí Objednávky budou akceptační kritéria, viz čl. IV odst. 4.8 pododst 4.8.13 Smlouvy, bude případný akceptační proces ukončen podpisem akceptačního protokolu, který bude reflektovat splnění či nesplnění akceptačních kritérií a bude podepsán Oprávněnými osobami obou Smluvních stran. Podrobný popis akceptačního procesu, tj. zejména lhůty pro akceptaci a proces odstraňování případných výhrad, bude vždy součástí příslušné Objednávky, v případě, že Objednávka bude obsahovat akceptační kritéria.

VI. CENA A PLATEBNÍ PODMÍNKY

6.1 Poskytovatel se zavazuje provádět jednotlivé Služby dle jednotlivých Objednávek uzavíraných dle této Smlouvy s Objednatelem nejvýše za ceny uvedené v příslušné Objednávce na Službu (dále jen „**Cena za Službu**" nebo společně „**Ceny za Služby**").

6.2 Přičemž Ceny za Služby dle čl. II odst. 2.4 pododst. 2.4.1, pododst. 2.4.2, pododst. 2.4.3, pododst. 2.4.4 (pouze v rozsahu Administrace SŘBI), pododst. 2.4.6 a pododst. 2.4.7 Smlouvy 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 na základě jednotkových cen uvedených v Příloze č. 13 Smlouvy, přičemž principy stanovení každé Ceny za Službu jsou uvedeny v Příloze č. 1 až Příloze č. 4 Smlouvy, Příloze č. 6 a Příloze č. 7 Smlouvy pro daný typ Služby.

6.3 Cena za Službu dle čl. II odst. 2.4 pododst. 2.4.4 Smlouvy v rozsahu Metodické podpory a pododst. 2.4.5 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. 13 Smlouvy * počet prokazatelně vynaložených člověkodnů na poskytování Konzultací nebo Metodické podpory 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 a/nebo Metodickou podporu v rámci příslušného kalendářního měsíce se sčítají dle vykázaného a Objednatelem schváleného času skutečně stráveného na poskytování Konzultací a/nebo Metodické podpory, přičemž Poskytovatelem může být účtován čas s přesností na 1/8 člověkodne.

6.4 Ceny za Služby stanovené na základě odst. 6.2 a 6.3 tohoto článku se zvýší o částku odpovídající dani z přidané hodnoty dle sazby daně platné ke dni uskutečnění zdanitelného plnění.

6.5 Poskytovatel prohlašuje, že je plátcem DPH.

6.6 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 400 000 000 Kč bez DPH (dále jen „**Maximální souhrnná cena**").

6.7 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. 6.6 tohoto článku Smlouvy. Současně se Smluvní strany zavazují, že v případě, kdy v průběhu plnění Objednávek uzavřených na poskytování Služeb dojde k požadavku Objednatele na změnu rozsahu poskytování jednotek daného typu Služby v rámci dané Objednávky a v důsledku toho by mělo dojít ke změně jednotkové ceny pro daný typ Služby v souladu s Přílohou č. 13 Smlouvy, uzavřou pro daný typ Služby novou Objednávku zahrnující i požadované změny jednotek pro daný typ Služby, která v plném rozsahu nahradí původní Objednávku.

6.8 Ceny za Služby dle příslušných Objednávek budou Objednatelem hrazeny měsíčně, a to na základě řádných daňových dokladů (faktur) vystavených Poskytovatelem zpětně za každý kalendářní měsíc poskytování Služeb v rámci všech trvajících Objednávek. Přičemž pro Služby dle čl. II odst. 2.4 pododst. 2.4.1, 2.4.2, 2.4.3, 2.4.4 (pouze v rozsahu Služby Administrace SŘBI), 2.4.6 a 2.4.7 Smlouvy je Poskytovatel oprávněn vystavit fakturu za daný kalendářní měsíc nejdříve v den akceptace Záznamu. Kopie akceptovaného Záznamu bude přílohou faktury. Pro Službu dle čl. II odst. 2.4 pododst. 2.4.4 Smlouvy (v rozsahu Metodické podpory) a pododst. 2.4.5 Smlouvy, tj. Konzultace je Poskytovatel oprávněn vystavit fakturu za daný kalendářní měsíc nejdříve v den akceptace Výkazu bez výhrad. 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, 2.4.2, 2.4.3, 2.4.4 (pouze v rozsahu Služby Administrace SŘBI), 2.4.6 a 2.4.7 Smlouvy, příp. pouze některá z nich, 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.

6.9 Faktura musí obsahovat zejména:

6.9.1 číslo Smlouvy;

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

6.9.3 specifikaci jednotlivých Služeb, které jsou fakturovány, příp. rovněž uvedení počtu člověkodnů, za které je fakturováno v případě faktury za Konzultace a/nebo Metodickou podporu;

6.9.4 Cenu za Službu, příp. Ceny za Služby v rámci všech trvajících Objednávek, bez DPH a s DPH;

6.9.5 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;

6.9.6 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;

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

6.10 Faktury jsou splatné ve lhůtě 30 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, 2.4.2, 2.4.3, 2.4.4 (pouze v rozsahu Služby Administrace SŘBI), 2.4.6 a 2.4.7 Smlouvy je poslední den kalendářního měsíce, ve kterém byly Služby poskytovány a pro Službu dle čl. II odst. 2.4. pododst. 2.4.4 Smlouvy (v rozsahu Metodické podpory) a pododst. 2.4.5 Smlouvy je datem uskutečnění zdanitelného plnění datum akceptace Výkazu bez výhrad.

6.11 Poskytovatel bude faktury doručovat prostřednictvím datové schránky Objednatele.

6.12 Objednatel je oprávněn ve lhůtě 15 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. 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 kalendářních dnů.

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

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

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

6.16 Poskytovatel je oprávněn zvýšit každou z Cen za Službu 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.

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

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

VII. ZMĚNOVÉ ŘÍZENÍ

7.1 Kterákoliv ze Smluvních stran je oprávněna na základě Zprávy písemně navrhnout změny Služeb a parametrů jejich poskytování v rámci příslušné Objednávky, a to prostřednictvím požadavku zaslaného prostřednictvím e-mailu nebo předaného na jednání TPP 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 Služeb z hlediska vhodnosti, termínů plnění, součinnosti Smluvních stran a ceny dle příslušné Objednávky. Poskytovatel se zavazuje provést hodnocení bez zbytečného odkladu, nejpozději do 10 pracovních dnů ode dne doručení Změnového požadavku Objednateli, 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 plnění Služeb, termíny plnění Služeb, cena Služeb, platební podmínky, součinnost Objednatele atd. Pro vyloučení pochybností Smluvní strany sjednávají, že dodatek uzavřený na základě tohoto článku ke Smlouvě nebo k Objednávce, resp. změny provedené tímto dodatkem jsou účinné od okamžiku účinnosti dodatku rovněž vůči všem Objednávkám trvajícím k okamžiku nabytí účinnosti dodatku.

7.4 Obě Smluvní strany se zavazují případné změny či doplňky této Smlouvy či Objednávky činit písemně v souladu s ustanoveními ZZVZ, eventuálně v souladu s jinými právními předpisy upravujícími zadávání veřejných zakázek, platnými a účinnými v době změny 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 až 4 a dále v Příloze č. 6 a Příloze č. 7 Smlouvy;

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

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

8.1.4 bez zbytečného odkladu oznámit Objednateli veškeré skutečnosti, které mohou mít vliv na povahu nebo na podmínky poskytování Služeb 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, a to nejpozději do 5 pracovních dnů od ukončení poslední Objednávky uzavřené na základě této Smlouvy, nedohodnou-li se Smluvní strany jinak;

8.1.8 seznámit každého ze svých zaměstnanců a zaměstnanců svého poddodavatele a jiných osob, které se budou podílet na plnění Služeb s povinnostmi vyplývajícími z interních předpisů a jiné dokumentace Objednatele, které upravují řízení bezpečnosti informací přímo souvisejícími s plněním Služeb. O seznámení každého jednotlivého zaměstnance nebo jiné osoby Poskytovatel vyhotoví záznam, jehož náležitosti určí Objednatel, a předá následně tento záznam Objednateli, a to před zahájením plnění Služeb dle příslušné Objednávky, resp. před zahájením činnosti konkrétním pracovníkem.

8.1.9 poskytnout Objednateli potřebnou součinnost při provádění kontroly a auditu kritické informační infrastruktury.

8.1.10 Poskytovatel tímto prohlašuje, že je pojištěn z titulu odpovědnosti za způsobenou škodu v souvislosti s poskytováním Služeb 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.

8.1.11 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 pracovních dnů od doručení písemné žádosti Objednatele. Nepředá-li Poskytovatel kopii aktuální pojistné smlouvy nebo pojistného certifikátu dle této Smlouvy, má se za to, že Poskytovatel není pojištěn ve smyslu tohoto článku Smlouvy.

8.2 Objednatel se zavazuje:

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

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

8.2.3 zaplatit za řádně poskytnuté Služby nebo jejich části cenu za Služby dle příslušné Objednávky.

8.2.4 seznámit Poskytovatele se svými interními předpisy a další dokumentací vztahující se přímo k plnění Služeb (viz pododst. 8.1.8), které upravují řízení bezpečnosti informací a dále je povinen k poskytnutí součinnosti při zodpovídání dotazů Poskytovatele v rámci seznámení s touto dokumentací.

8.3 Poskytovatel se zavazuje dodržovat relevantní ustanovení ZoKB, VoKB a ZoZOU dle charakteru Služeb popsaných v Příloze č. 1 až Příloze č. 7 Smlouvy.

IX. PODDODAVATELÉ

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

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

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 Služeb, bezpečnosti a ochrany zdraví při práci, ochrany životního prostředí, likvidace odpadů a norem systému řízení bezpečnosti informací.

10.4 Komunikace mezi Smluvními stranami, související s řízením poskytování Služeb, bude probíhat prostřednictvím Řídicích orgánů, popř. jimi pověřených osob. Popis činností Řídicích orgánů, jejich odpovědnosti a kompetence jsou uvedeny v Příloze č. 8 Smlouvy.

10.5 Smluvní strany se zavazují, že do 3 pracovních dnů od účinnosti Smlouvy jmenují své zástupce do Řídicích orgánů. Oprávněné osoby Smluvních stran jsou oprávněny jednostranně změnit zástupce jmenované do Řídicích orgánů bez nutnosti uzavření dodatku ke Smlouvě. V takovém případě jsou povinny na takovou změnu druhou Smluvní stranu předem písemně upozornit, jinak tato změna nemá vůči druhé Smluvní straně právní účinky. Oprávněná osoba Objednatele se zavazuje vést aktuální seznam členů Řídicích orgánů a na vyžádání jej předložit Oprávněné osobě Poskytovatele.

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

XI. NÁHRADA ÚJMY

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

11.2 Poskytovatel odpovídá za každé zaviněné porušení povinnosti.

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

11.4 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.

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

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

XII. ODPOVĚDNOST ZA VADY

12.1 Poskytovatel je povinen poskytovat Služby v souladu s požadavky a při dodržení povinností sjednaných v této Smlouvě a dané Objednávce. Objednatel je povinen řádně poskytnuté Služby 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 veškeré návody, rady a doporučení, které v souvislosti s poskytováním Služby Objednateli zpřístupnil, vychází z nejaktuálnějších informací, které bylo možné získat na českém trhu.

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

12.5 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 (s výjimkou termínu stanoveného pro zahájení poskytování Služby), pokud byl v rámci dané Objednávky harmonogram sjednán nebo v případě nedodržení termínů stanovených v rámci akceptace dle čl. V odst. 5.2.2 Smlouvy, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 5 000 Kč (slovy: pět tisíc korun českých) za každý i započatý 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. 8.1.10 Smlouvy, má Objednatel právo uplatnit vůči Poskytovateli smluvní pokutu ve výši 50 000 Kč (slovy: padesát tisíc korun českých), a to za každý započatý kalendářní den prodlení.

13.3 V případě, že některá ze Smluvních stran poruší některou z povinností mlčenlivosti dle čl. XV této Smlouvy, je druhá Smluvní strana oprávněna požadovat smluvní pokutu ve výši 250 000 Kč (slovy: dvě stě padesát tisíc korun českých), a to každý jednotlivý případ porušení.

13.4 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 Kč (slovy: jedno sto tisíc korun českých), a to každý jednotlivý případ porušení.

13.5 V případě, že Poskytovatel nesplní některou ze stanovených SLA povinností, tj. stanovené dostupnosti příslušné Služby v Příloze č. 1 až v Příloze č. 4 (v případě Přílohy č. 4 pouze v rozsahu Služby Administrace SŘBI) a Příloze č. 6 a Příloze č. 7 Smlouvy, 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.

13.6 V případě prodlení Poskytovatele s odstraněním závady příslušné Služby ve lhůtě stanovené v Příloze č. 1 nebo Příloze č. 2 nebo Příloze č. 3 nebo Příloze č. 4 (v případě Přílohy č. 4 pouze v rozsahu Služby Administrace SŘBI) nebo Příloze č. 6 nebo Příloze č. 7 Smlouvy, 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.

13.7 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 Kč (slovy: pět tisíc korun českých), a to za každý i započatý den prodlení.

13.8 V případě, že Poskytovatel nepředá Objednateli ke schválení Nabídku v termínu uvedeném v čl. IV odst. 4.4 Smlouvy, je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 5 000 Kč (slovy: pět tisíc korun českých) za každý i započatý den prodlení.

13.9 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 15 000 Kč (slovy: patnáct tisíc korun českých) za každý i započatý den prodlení.

13.10 V případě, že Poskytovatel nedodrží termín pro vyhotovení Exit plánu stanovený v předmětné Objednávce v souladu s čl. XVI odst. 16.12 Smlouvy, je povinen Poskytovatel uhradit Objednateli smluvní pokutu ve výši 15 000 Kč (slovy: patnáct tisíc korun českých) za každé jednotlivé porušení této povinnosti.

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

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

13.13 Ujednáním o smluvní pokutě není dotčeno právo poškozené Smluvní strany domáhat se náhrady újmy v mezích dle čl. XI. odst. 11.4. Smlouvy.

13.14 Aniž by byl dotčen předcházející odstavec, Smluvní strany se výslovně dohodly, že celková výše všech nároků na smluvní pokuty vzniklých na základě nebo v souvislosti s touto Smlouvou, resp. jednotlivými Objednávkami jedné Smluvní straně se omezuje celkovou částkou 200 000 000 Kč (slovy: dvě stě milionů korun českých).

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

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 Služby;

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. Pro vyloučení pochybností Smluvní strany uvádějí, že Poskytovatel i Objednatel jsou následně oprávněni Autorské dílo zveřejnit;

14.1.5 Objednatel (nabyvatel licence) není povinen licenci využít;

14.1.6 Objednatel (nabyvatel licence) je oprávněn bez dalšího práva tvořící 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. 6 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 Služby podle čl. VI Smlouvy.

14.3 V případě, že součástí plnění Poskytovatele podle této Smlouvy jsou movité věci, 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 Služby dle předmětné Objednávky.

XV. MLČENLIVOST A OCHRANA INFORMACÍ SMLUVNÍCH STRAN

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

15.1.1 veškeré informace poskytnuté si Smluvními stranami v souvislosti s plněním této Smlouvy či Objednávek (pokud nejsou výslovně obsaženy ve znění Smlouvy či Objednávky zveřejňovaném dle čl. XVIII odst. 18.1.);

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

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

15.2 Povinnost zachovávat mlčenlivost uvedená v odst. 15.1 tohoto článku se nevztahuje na informace:

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

15.2.2 jejichž sdělení vyžaduje jiný právní předpis;

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

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

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

15.3 Jako s Neveřejnými informacemi musí být nakládáno také s informacemi, které splňují podmínky uvedené v odst. 15.1 tohoto článku, i když byly získány náhodně nebo bez vědomí druhé Smluvní strany a dále s veškerými informacemi získanými od jakékoliv třetí strany, pokud se týkají Smluvní strany nebo plnění této Smlouvy či Objednávek.

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

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

15.6 Povinnost mlčenlivosti dle této Smlouvy trvá i po naplnění této Smlouvy bez ohledu na zánik ostatních závazků ze Smlouvy, a to v případě Neveřejných informací po dobu 10 let ode dne ukončení poslední Objednávky uzavřené na základě této Smlouvy a v případě obchodního tajemství po dobu existence obchodního tajemství, pokud nebude povinnosti mlčenlivosti dříve daná Smluvní strana druhou Smluvní stranou písemně zproštěna.

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

15.8 Smluvní strany berou na vědomí, že vzhledem k tomu, že s plněním této Smlouvy je spojeno zpracování osobních údajů pracovníků Objednatele a případně rovněž dodavatelů Objednatele – podnikajících fyzických osob, které poskytují Objednateli v rámci pracovněprávních a obchodních vztahů (dále jen „**Osobní údaje**") ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „**Obecné nařízení**"), je pro účely této Smlouvy Objednatel v postavení správce Osobních údajů (pro účely odst. 15.8 a 15.9 Smlouvy dále jen „**Správce**") a Poskytovatel v postavení zpracovatele Osobních údajů (pro účely odst. 15.8 a 15.9 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 a dle ZoZOU, jakožto prováděcího předpisu k Obecnému nařízení a příslušných právních předpisů.

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

XVI. DOBA TRVÁNÍ A UKONČENÍ SMLOUVY

16.1 Tato Smlouva se uzavírá na dobu určitou, a to od okamžiku účinnosti Smlouvy, tj. od okamžiku zveřejnění Smlouvy v registru smluv v souladu se Zákonem o registru smluv na dobu 48 měsíců nebo do okamžiku, kdy celková hodnota plnění uzavřených Objednávek dosáhne Maximální souhrnné ceny, podle toho, která ze skutečností nastane dříve.

16.2 Smlouva a 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 zveřejnění 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 měsíců a počíná běžet prvním dnem měsíce následujícího po měsíci, ve kterém bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé Smluvní straně. Výpovědní doba každé Objednávky činí 4 měsíců a počíná běžet prvním 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 daného plnění (v případě, že byl v rámci Objednávky požadován), a to do 30 dnů od doručení výpovědi Objednateli.

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

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 ani 15 kalendářních dnů po obdržení písemného oznámení Objednatele napravit, 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 ani 30 kalendářních dnů po obdržení písemného oznámení Objednatele napravit,

16.6.3 porušení povinnosti mlčenlivosti, resp. ochrany důvěrných informací Poskytovatelem,

16.6.4 poskytování Služeb dle Objednávky je bezdůvodně pozastaveno po dobu více než 30 kalendářních dnů.

16.7 Objednatel je dále oprávněn bez jakýchkoliv sankcí vůči jeho 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 pověří plněním některých povinností z této Smlouvy třetí stranu bez předchozího informování Objednatele;

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

16.7.4 bez předchozího písemného souhlasu Objednatele dojde k převodu, byť i jen části, závazků plynoucích z této Smlouvy na třetí osobu, a to z jakéhokoliv důvodu (vč. převodu podniku nebo jeho části na třetí osobu);

16.7.5 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;

16.7.6 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;

16.7.7 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;

16.7.8 Poskytovatel vstoupí do likvidace;

16.7.9 dojde k významné změně kontroly nad Poskytovatelem, přičemž kontrolou se zde rozumí vliv, ovládání či řízení dle ust. § 71 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) (dále jen „**ZOK**"), či ekvivalentní postavení. Nastane-li případ dle předcházející věty, je Poskytovatel povinen informovat o této skutečnosti Objednatele písemně do 2 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 (tj. ex nunc). Smluvní strany si jsou povinny vyrovnat dosavadní vzájemné závazky ze Smlouvy, příp. Objednávky, a to bez zbytečného odkladu, nejpozději však do 30 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 kalendářních dnů a dále v případě, že Poskytovateli nebude Objednatelem poskytována součinnost v souladu s touto Smlouvou, a to ani přes výzvu Poskytovatele k nápravě.

16.10 Dosáhne-li plnění z této Smlouvy takové výše, že Služby není možné provést bez překročení Maximální souhrnné ceny, má každá Smluvní strana právo od Smlouvy odstoupit. Ustanovení odst. 16.11 tohoto článku se použije obdobně.

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

16.12 Poskytovatel se zavazuje vyhotovit v termínu uvedeném v příslušné Objednávce exit plán, který bude obsahovat postup provádění činností provozního a dokumentačního charakteru, včetně předávání znalostí, souvisejících s předmětem a rozsahem Služeb dle dané Objednávky (dále jen „**Exit plán**").

16.13 Ukončením Smlouvy, jakož i Objednávek nejsou dotčena práva na zaplacení smluvní pokuty nebo zákonného úroku z prodlení, pokud už dospěl, práva na náhradu škody, práva a povinnosti vyplývající z čl. XV Smlouvy, práva z odpovědnosti za vady 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. 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, poštou, prostřednictvím datové schránky či kurýrem na adresy uvedené v tomto odstavci (včetně označení jménem příslušné Oprávněné osoby) nebo na jinou adresu, kterou příslušná Smluvní strana v předstihu písemně oznámí adresátovi, není-li v konkrétním případě stanoveno ve Smlouvě jinak:

17.1.1 Objednatel:

Název: Česká republika – Generální finanční ředitelství
Adresa: Lazarská 15/7, 117 22 Praha 1
K rukám: jméno Oprávněné osoby Objednatele
Datová schránka: p9iwj4f

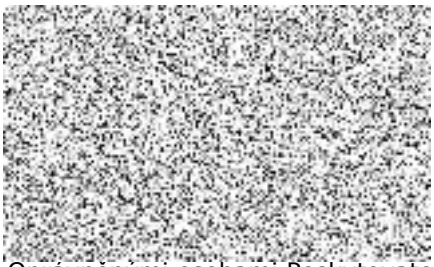
17.1.2 Poskytovatel:

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

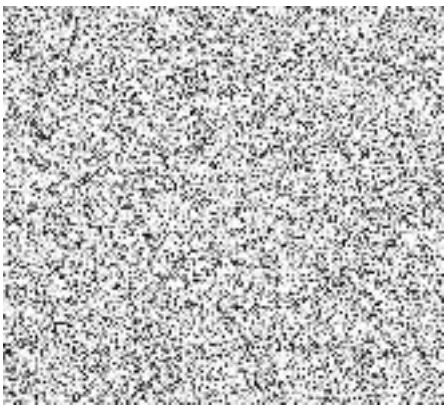
17.2 Účinnost oznámení nastává v pracovní den následující po dni doručení tohoto oznámení druhé Smluvní straně, není-li ve Smlouvě nebo Objednávce v konkrétním případě stanoveno jinak.

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. V případě, že Smluvní strana má více Oprávněných osob, zasílají se veškeré e-mailové zprávy na adresy všech oprávněných osob v kopii:

17.3.1 Oprávněnými osobami Objednatele jsou:



17.3.2 Oprávněnými osobami Poskytovatele jsou:



17.4 Ke změně nebo ukončení Smlouvy, k uzavření, změně nebo ukončení Objednávky je za Objednatele oprávněn generální ředitel a dále osoby pověřené generálním ředitelem. 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.

XVIII. ZÁVĚREČNÁ USTANOVENÍ

18.1 Obě Smluvní strany souhlasí s tím, že podepsaná Smlouva (včetně příloh) a Objednávky (vč. případných příloh), jakož i jejich text, můžou být v elektronické formě zveřejněny v souladu s povinnostmi vyplývajícími z právních předpisů, a to bez časového omezení. Objednatel 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 vč. 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 dnů ode dne zahájení jednání o dohodě, bude předmětný spor rozhodován s konečnou platností před věcně a místně příslušným soudem České republiky, přičemž rozhodným právem je právo české.

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 Nedílnou součástí této Smlouvy jsou tyto přílohy:

Příloha č. 1: Bezpečnostní monitoring

Příloha č. 2: Log management

Příloha č. 3: Správa privilegovaných účtů

Příloha č. 4: KCKB

Příloha č. 5: Konzultace v oblasti informační a kybernetické bezpečnosti

Příloha č. 6: Vulnerability management

Příloha č. 7: Správa syslog serverů

Příloha č. 8: Řízení poskytování Služby

Příloha č. 9: Vzor Nabídky

Příloha č. 10: Vzor Objednávky

Příloha č. 11: Vzor Záznamu

Příloha č. 12: Vzor Zprávy

Příloha č. 13: Jednotkové ceny pro Služby

Za Objednatele:
V Praze dne dle el. podpisu

generální ředitelka
Česká republika – Generální finanční ředitelství

Za Poskytovatele:
V Praze dne dle el. podpisu

1. zástupce generálního ředitele
Státní pokladna Centrum sdílených služeb, s. p.

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
Ukončení poskytování Služby KL01	Na základě Objednávky

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 dodané Objednatelem pro Službu KL01 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.

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 ve smyslu Security Operations Center (jako jedna z komponent, které jsou dále rozepsány v jednotlivých katalogových listech souvisejících služeb) 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.

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 lepšování 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 funkcí, 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.

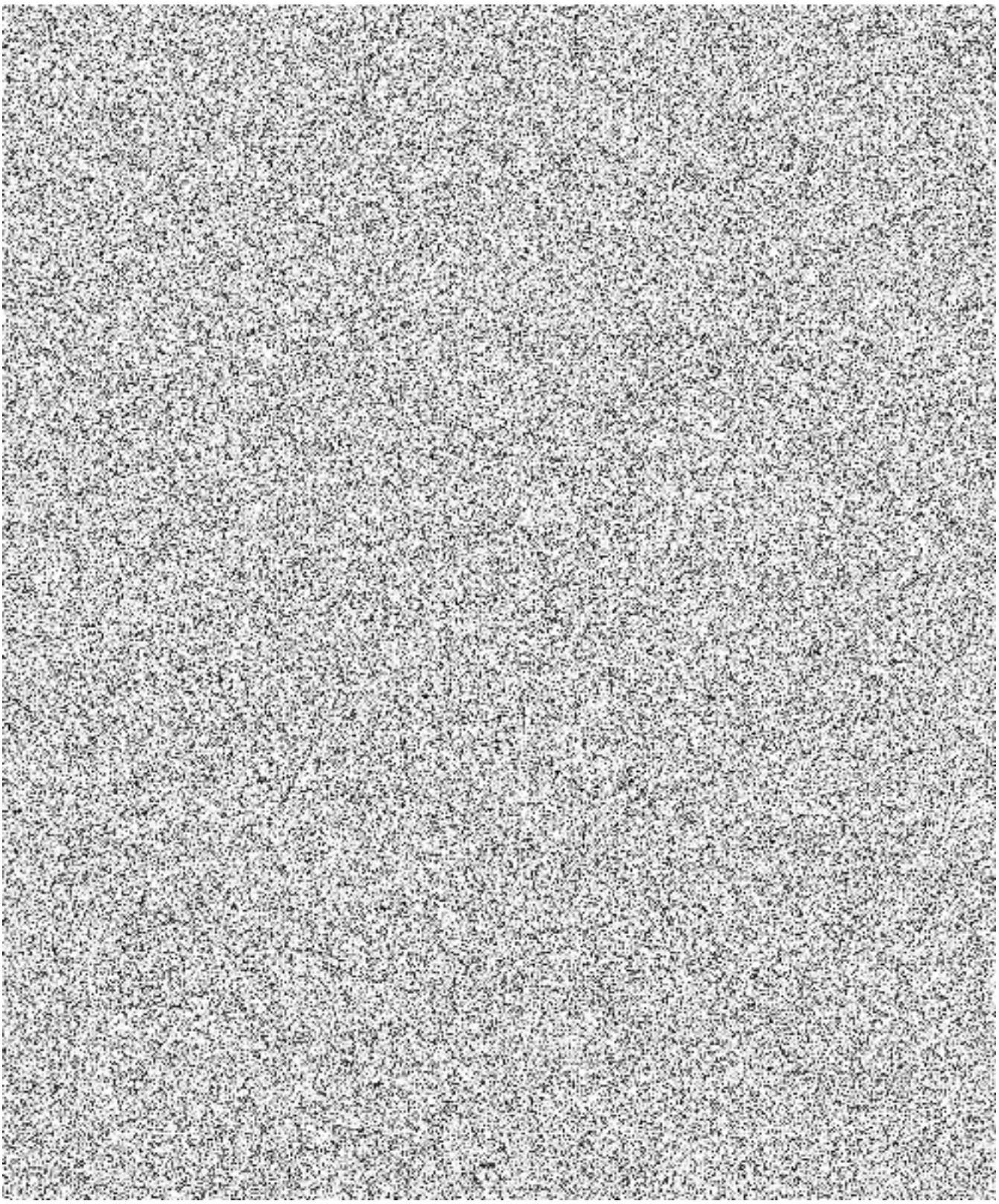
6.4 PLÁNOVANÉ ODSTÁVKY

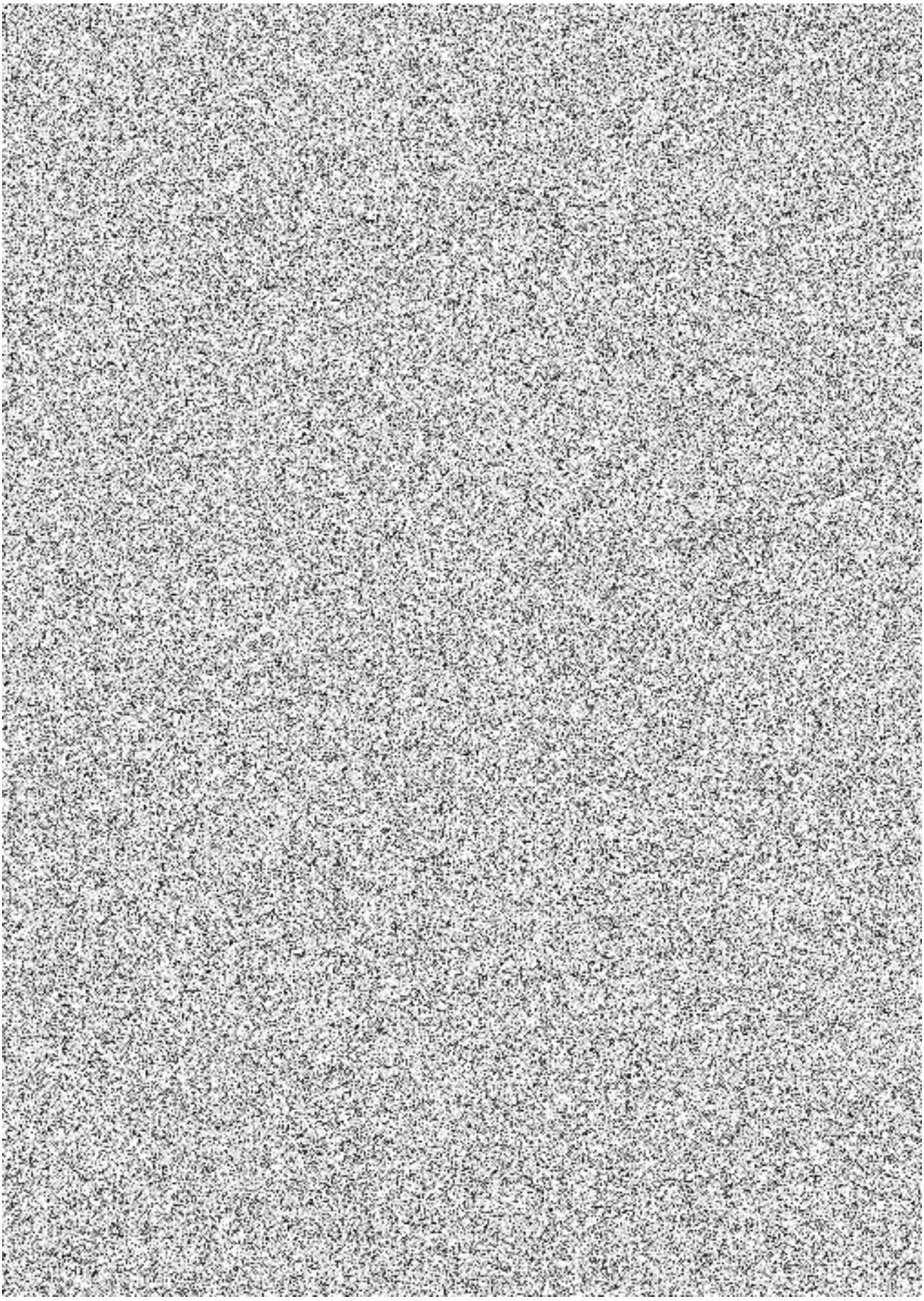
V rámci poskytování Služby KL01 si Poskytovatel vyhrazuje právo na plánované odstávky celého nebo částí systému z důvodu údržby jak samotného systému, tak infrastruktury a datové konektivity Poskytovatele. Poskytovatel se zavazuje plánované práce s vlivem na dostupnost Služby KL01 soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL01 ovlivněna co nejméně.

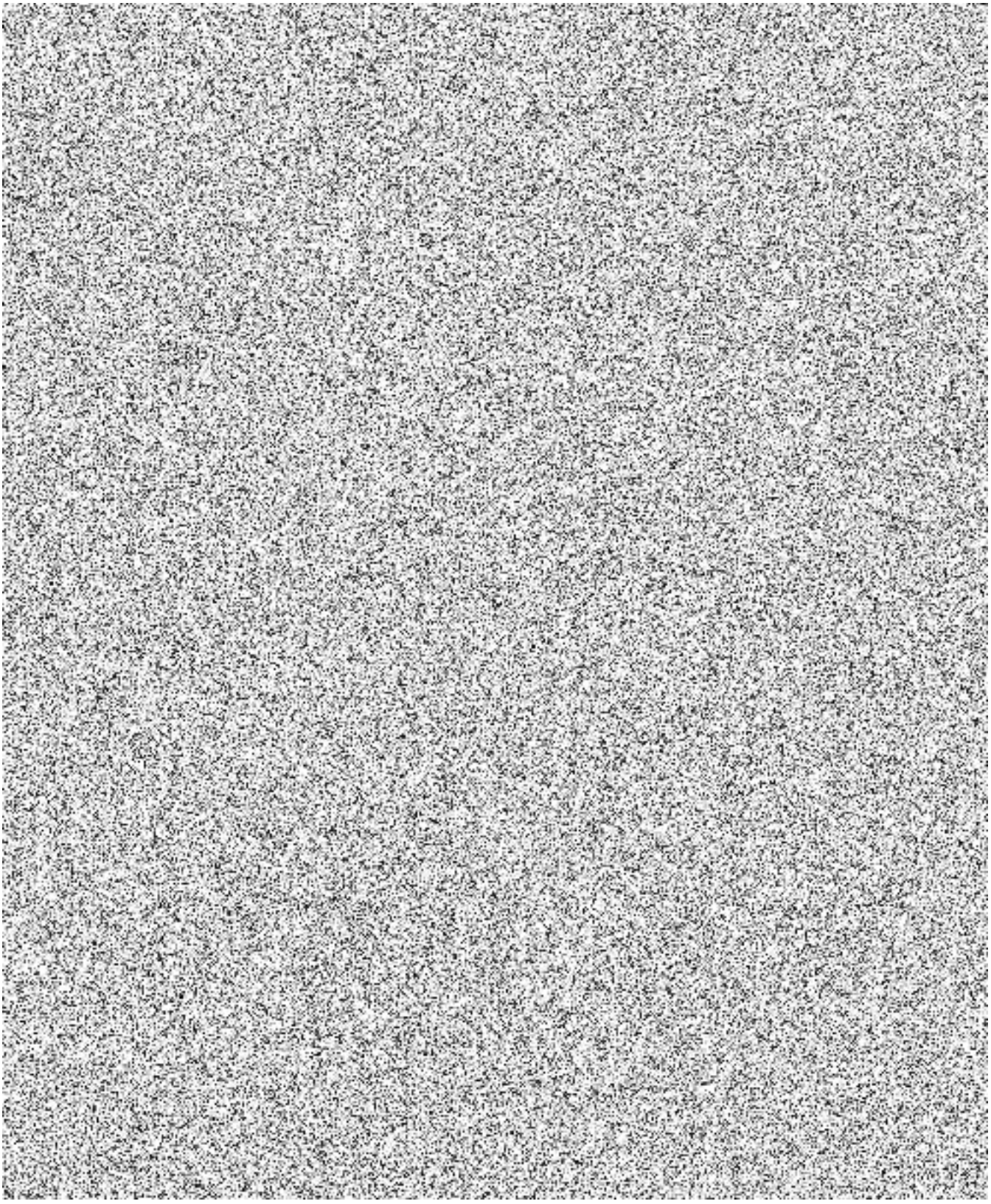
Plánované odstávky jsou, pokud možno, soustředěny do servisních oken, která jsou každý čtvrtek v čase 19:00 až 24:00. Ve výjimečných případech jsou odstávky Služby KL01 ohlašovány a realizovány i mimo tato servisní okna. Doba odstávky, která byla předem řádně ohlášena se nezapočítává do nedostupnosti 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.







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 Přílohou č. 13 Smlouvy a 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 analýza bude stanoveno množství jednotek pro zajištění řádného poskytování Služby KL01. Výsledná cena Služby KL01 se stanoví jako součin množství požadovaných jednotek a jejich jednotkové ceny uvedené v Příloze č. 13 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:

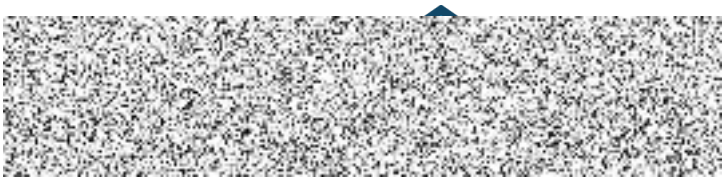
- zpracování dokumentu „Závěrečná zpráva analýzy řešení bezpečnostního monitoringu v rozsahu informačního systému Objednatele".

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

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 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)	VIS je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.
ZoKB	Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
VoKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
Významná 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.

Výraz	Popis
	• 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.
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.

Výraz	Popis
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	**Log management**

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Log management (dále v tomto katalogovém listu jen „**Služba KL02**") je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL02.

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

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba KL02 bude poskytována v režimu, jak je uvedeno v tabulce níže:

Režim poskytování Služby KL02	Doba poskytování Služby KL02
Standardní provozní doba	Nepřetržitě (24x7)

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 VSTUPY

Vstupy dodané Objednatelem pro Službu KL02 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 KL02 jsou:

- Testování a nasazení Služby KL02;
- Poskytování Služby KL02;
- měsíční zpráva o stavu služby dle tohoto katalogového listu;
- dokument Nasazení Služby KL02 v rozsahu Objednávky Objednatele;

Na vyžádání jsou Objednateli poskytovány informace v souladu s tímto katalogovým listem, které musí být předány bez zbytečného odkladu.

4 POPIS ROZSAHU SLUŽBY

Služba KL02 je ucelené řešení pro pokrytí potřeb Log managementu a zpracování logů pro vizualizaci a sledování logů vybraných zařízení, operačních systémů, aktivních síťových zařízení, platforem pro provoz aplikací, databází a aplikací. Služba KL02 je provozována v prostředí Poskytovatele.

Služba KL02 je poskytována v následujícím rozsahu:

- centrální sběr logů z příslušných systémů/zdrojů GFŘ v dojednaném denním objemu a s dohodnutým výkonem za sekundu a jejich indexaci;
- uložení logů s retencí 18 měsíců nebo volitelně;
- zálohování dat; retence zálohování bude definována;
- přístup a vyhledávání v uložených datech pracovníky Objednatele;
- preprocessing pro Službu KL01 dle Přílohy č. 1 Smlouvy;
- vizualizace dat.

Část 1 - Standardní součásti Služby KL02 (nedílné součásti KL02, poskytováno vždy)	
☒	Centrální sběr logů
☒	Uložení logů s definovanou retencí
☒	Zálohování logů
☒	Přístup a vyhledávání v uložených datech
☒	Vizualizace dat

V rámci Služby KL02 je pokryta vybraná povinnost definovaná 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"), a to:

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

Služba KL02 zaznamenává logy včetně jejich bezpečného uchovávání po dobu požadovanou VoKB.

Součástí Služby KL02 není tvorba dokumentace, vyjma dokumentace dle kapitoly 3 tohoto katalogového listu.

5 POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL02

Předmětem Služby KL02 je nepřetržité ukládání protokolů událostí (dále také „logy") v režimu 24x7 z rozsahu definovaných aktiv Objednatele. Zdrojem logů mohou být aktivní síťové prvky, operační systémy, platformy pro provoz aplikací, databáze, aplikace a bezpečnostní zařízení.

Komunikace z definovaných aktiv probíhá pomocí vynuceného zabezpečené komunikace, s podporou komunikačního protokolu TLS v aktuální doporučované bezpečné verzi. Napojení aktiv, které nemají možnost zabezpečené formy přenosu dat do služby Log managementu, je řešeno pomocí agregačních prvků Log managementu, které jsou umístěny co nejblíže zdroji. Tyto agregační body pak šifrovaně komunikují s centrálním systémem Log Managementu.

Přístup uživatelů a správců ke službě je řízen. Služba umožňuje přístup pouze oprávněným osobám a zajišťuje granulární ochranu pomocí přístupových oprávnění až do úrovně ochrany jednotlivých polí v objektu. Zabezpečení dat pokrývá viditelnost dat, viditelnost jednotlivých atributů, čtení a zápis dat nebo zamezení jejich změny.

Služba pracuje v režimu vysoké dostupnosti. Záloha je zajištěna pomocí vzdáleného úložiště a umožňuje jednoduchou obnovu dat. Služba KL02 tvoří komplexní funkční celek se službou Bezpečnostní monitoring KL01.

Služba KL02 logy shromažďuje, sjednocuje a zajišťuje jejich dlouhodobé zabezpečené uchovávání v distribuované storage.

Služba KL02 zajišťuje:

- bezpečnost a integritu záznamů (ochrana před zneužitím, změněním nebo vymazáním) napříč celým log management systémem podle možné závažnosti zneužití;
- zachování věrohodnosti a nezpochybnitelnosti záznamů;
- vytvoření dostatečně univerzální platformy centrálního log managementu.

Data jsou ukládána a zpracovávána s nejvyšší možnou úrovní zabezpečení v infrastruktuře SPCSS, která je provozována v souladu se standardy ISO 27001 a ZoKB.

Součástí služby je i webové prostředí, které umožňuje uložená data vizualizovat, ale i vyhledávat. Pro vytváření přehledů lze využít grafy, tabulky.

6 SLA PARAMETRY

Poskytovatel je povinen poskytovat službu KL02 dle Smlouvy v rozsahu definované objednávkou, a to v níže uvedených parametrech.

Ovlivnění chodu všech částí Služby KL02 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 KL02.

6.1 POŽADOVANÁ ROČNÍ DOSTUPNOST ČÁSTÍ SLUŽBY – ČÁST 1

Název Služby	**Log management**	
SLA parametry		
Část Služby	**Dostupnost Služby**	**Servisní okno pro odstávky**
Část 1 – Centrální sběr logů, Uložení logů s definovanou retencí, Přístup a vyhledávání v datech, Vizualizace dat	99,5 % při současném zachování 99,9 % logů	každý čtvrtek, vždy 19:00-24:00

Tabulka: Služba KL02 – Část 1

Servisní okno (časově definované v tabulce) není započteno do Dostupnosti služby.

Nedostupnost Služby KL02 – Část 1 (Centrální sběr logů, Uložení logů s definovanou retencí, Zálohování logů, Přístup a vyhledávání v datech, Vizualizace dat) způsobená hardwarovou nebo jinou technickou závadou se počítá od okamžiku zahájení nedostupnosti Služby KL02 – Část 1 ve výše definovaném rozsahu do okamžiku obnovení poskytování. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti Služby KL02 – Část 1 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).

Název Služby	Log management
SLA parametry	
Režim poskytování Služby KL02	**Hodnota**
Roční dostupnost	99,5 % při současném zachování 99,9 % logů

Tabulka: Roční dostupnost služby KL02

Dostupnost je měřená ročně, a to od 00:00 hod. 1. 1. do 24:00 hod. 31. 12. každého kalendářního roku. Na počátku každého kalendářního roku Poskytovatel vypočítá maximální možné trvání nedostupnosti Služby KL02 pro dané období podle uvedených procentuálních hodnot požadované roční dostupnosti.

Po dobu vyřešení incidentu jsou logy Poskytovatelem ukládány lokálně a následně zpětným importem nahrány do poskytované platformní služby.

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 dle specifické Části Služby KL02.

6.1.2. POŽADOVANÉ LHŮTY PRO OBNOVENÍ SLUŽBY KL02 – ČÁST 1

Název Služby	Log management		
Část Služby	**Lhůta pro obnovení služby v běžné provozní době v hodinách**		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Část 1 – Centrální sběr logů, Uložení logů s definovanou retencí, Zálohování logů, Přístup a vyhledávání v datech, Vizualizace dat	24	36	168

Tabulka: Požadované lhůty pro obnovení Služby KL02 – Části 1

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) její běžný provoz.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

Tabulka: Kategorizace provozních incidentů

6.2 PLÁNOVANÉ ODSTÁVKY

V rámci poskytování Služby KL02 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 KL02 soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL02 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 KL02 ohlašovány i mimo tato servisní okna. Doba odstávky, která byla předem řádně ohlášena se nezapočítává do nedostupnosti Služby KL02. Za ohlášení se považuje informování určených osob Objednatele e-mailem, a to minimálně 24 h před zahájením mimořádné odstávky. Doba odstávky, která byla předem řádně ohlášena, se nezapočítává do nedostupnosti Služby KL02. Ovlivnění chodu Služby KL02 ze strany Objednatele se nezapočítává do nedostupnosti Služby KL02.

Poskytovatel připraví čtvrtletní plán odstávek, který bude obsahovat jaké odstávky a pro jakou činnost jsou plánované. Tento plán odstávek Poskytovatel předá oprávněné osobě Objednatele, které bude tento dokument sloužit pro informativní účely. Tento plán odstávek bude předán před započetím čtvrtletí daného plánu. Čtvrtletní plán odstávek se může měnit na základě požadavků vzniklých z provozu dané Služby KL02. Projednání plánu odstávek bude předmětem pravidelného jednání Status.

7 SOUČINNOST PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY

Objednatel stanoví seznam určených osob pro plnění Služby KL02, tento seznam předá Poskytovateli do 5 pracovních dnů od účinnosti příslušné Objednávky. Objednatel je povinen každou změnu určených osob prokazatelně oznámit Poskytovateli.

8 PRINCIP STANOVENÍ CENY

Cena bude stanovena v souladu s Přílohou č. 13 Smlouvy a na základě požadavku Objednatele specifikovaného v Objednávce a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy pro následné poskytování Služby KL02.

Vstupní analýza bude použita pro stanovení množství jednotek pro zajištění řádného poskytování Služby KL02. Měsíční (paušální) cena Služby KL02 se stanoví jako součin množství požadovaných jednotek a jejich jednotkové ceny uvedené v Příloze č. 13 Smlouvy v daném kalendářním měsíci.

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 KL02, kdy je rozhodné naplnění zpracování dílčího plnění dle výše zmíněné Rámcové smlouvy, a to:

- zpracování dokumentu „Návrh řešení provozních a bezpečnostních monitoringů ICT systémů GFŘ v rozsahu vybraného ICT".

Služby Vstupní analýza není předmětem plnění Služby KL02.

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

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 KL02.

Služba Vstupní analýza a Realizace ověření provozu není samostatným Výstupem plnění Služby KL02 dle kapitoly 3.2. Tyto služby mohou být realizovány na základě samostatné objednávky dílčích částí Služby KL02 a KL05 (Konzultace).

9 POUŽITÉ VÝRAZY

Výraz	Popis
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)

KATALOGOVÝ LIST č. 03	
Název služby	**Správa privilegovaných účtů**

1. OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Správa privilegovaných účtů (dále jen **„Služba KL03"**) je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL03.

Název milníku	Termín splnění milníku
Zahájení poskytování Služby KL03	Na základě Objednávky
Ukončení poskytování Služby KL03	Na základě Objednávky

2. REŽIM POSKYTOVÁNÍ SLUŽBY

Služba KL03 bude poskytována v režimu, dle popisu v tabulce:

Režim poskytování Služby KL03	Doba poskytování Služby KL03
Standardní provozní doba – Část 1 a 2	Nepřetržitě (24x7)
Poskytování podpory Služby KL03	V pracovní dny (5x8) 8–16 h

3. VSTUPY A VÝSTUPY SLUŽBY

3.1. Vstupy

Vstupy dodané Objednatelem pro Službu KL03 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 KL03 jsou:

- Poskytování Služby KL03;
- 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 KL03 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 KL03 (nedílné součásti KL03, 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 KL03 nezahrnuje organizační opatření SŘBI Objednatele. Součástí Služby KL03 dle tohoto katalogového listu není tvorba politik.

5. POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL03

5.1. Řízení přístupu

Jedná se o klíčový modul pro řízení životního cyklu privilegovaného uživatele v dané organizaci Objednatele. 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 uživatelů, s indexovaným video log záznamy, všech nebo vybraných relací. Session recording lze využít na lokální aktivity uživatelů, 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 uživatelské relace uskutečňovány. Session recording nijak neomezuje práci uživatelů a nevyžaduje žádné změny organizačních procesů.

Monitoring probíhá v reálném čase a podezřelé aktivity ihned notifikuje. Uživatele, 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 uživatelů, 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 KL03

Jedná se o poskytování podpory související s poskytováním Služby KL03. 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 KL03;
- Režim poskytování Služby KL03;
- Popis rozsahu Služby KL03;
- Provozovaná prostředí;

- Aktivity Služby KL03;
- Řízení provozu Služby KL03;
- Návrh na nápravná opatření a doporučení.

7. SLA PARAMETRY

Poskytovatel je povinen poskytovat službu KL03 dle Smlouvy v rozsahu definované objednávkou, a to v níže uvedených parametrech.

Ovlivnění chodu všech částí Služby KL03 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 KL03.

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
Část 2 - Password Management	99,5 %	každý čtvrtek, vždy 19:00-24:00

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

Nedostupnost Služby KL03 – 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 KL03 – Část 1 a Část 2 ve výše definovaném rozsahu do okamžiku obnovení poskytování z pohledu objednavatele. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti Služby KL03 – 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 KL03.

7.1.2. POŽADOVANÉ LHŮTY PRO OBNOVENÍ SLUŽBY KL03 – VYBRANÁ ČÁST ČÁSTI 1 A ČÁST 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 KL03 – 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 KL03

Podpora dle Služby KL03 je určena k zajištění rozvoje a podpory jejího efektivního využívání. Doba reakce na požadovanou podporu Služby KL03 je počítána od zadání požadavku do aplikace Service Desk Poskytovatele. Za reakci je považována odpověď na požadavek s návrhem dalšího postupu řešení.

Podpora Služby KL03 je poskytována v režimu 8x5.

Název Služby	Správa privilegovaných účtů	
SLA parametry		
Část Služby	Maximální doba reakce na požadavek Objednatele	Doba vyřešení požadavku
Podpora Služby KL03 – Správa privilegovaných účtů (podpora 5x8)	Do 24 hodin od doby přijetí požadavku	Do 24 hodin od doby reakce na požadavek

Tabulka č. 2 – Reakční doby a doby podpory Služby KL03

Při přijetí požadavku dává Poskytovatel základní zpětnou vazbu.

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.

Maximální doba pro vyřešení požadavku 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. Maximální doba vyřešení požadavku může být pozastavena na základě oprávněného požadavku ze strany Poskytovatele.

7.3. Plánované odstávky

V rámci poskytování Služby KL03 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 KL03 soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL03 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 KL03 ohlašovány a realizovány i mimo tato servisní okna. Za ohlášení se považuje informování určených osob Objednatele e-mailem, a to minimálně 24 h před zahájením mimořádné odstávky. Doba odstávky, která byla předem řádně ohlášena, se nezapočítává do nedostupnosti Služby KL03. Ovlivnění chodu Služby KL03 ze strany Objednatele se nezapočítává do nedostupnosti Služby KL03.

Poskytovatel připraví čtvrtletní plán odstávek, který bude obsahovat jaké odstávky a pro jakou činnost jsou plánované. Tento plán odstávek Poskytovatel předá oprávněné osobě Objednatele, které bude tento dokument sloužit pro informativní účely. Tento plán odstávek bude předán před započetím čtvrtletí daného plánu. Čtvrtletní plán odstávek se může měnit na základě požadavků vzniklých z provozu dané Služby KL03. Projednání plánu odstávek bude předmětem pravidelného jednání Status.

8. SOUČINNOST PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY KL03

- Objednatel stanoví seznam určených osob pro plnění služby KL03, tento seznam předá Poskytovateli do 5 pracovních dnů od účinnosti příslušné Objednávky. Objednatel je povinen každou změnu určených osob prokazatelně oznámit Poskytovateli.
- Požadavky na podporu v rámci služby Správa privilegovaných účtů jsou Objednatelem zadávány pomocí Service Desku SPCSS Oprávněnou osobou nebo určenou osobou.

8. PRINCIP STANOVENÍ CENY

Cena bude stanovena v souladu s Přílohou č. 13 Smlouvy a na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy a následné Realizace ověření provozu pro následné poskytování Služby KL03.

Vstupní analýza bude použita pro návrh testovacího provozu, který bude ověřen při Realizaci ověření provozu, kde budou nastavena a ověřena technická řešení a procesy a budou stanovena množství jednotek pro zajištění řádného poskytování Služby KL03.

Výsledná cena Služby KL03 se stanoví jako součin množství požadovaných jednotek a jejich jednotkové ceny uvedené v Příloze č. 13 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 KL03, 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 KL03, 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 KL03 dle kapitoly 3.2. Tyto služby mohou být realizovány na základě samostatné objednávky dílčích částí Služby KL03 a KL05 (Konzultace).

9. 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. 04	
Název služby	**KCKB**

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Kompetenční centrum kybernetické bezpečnosti (dále také **„Služba KL04"**) je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL04.

Název milníku	Termín splnění milníku
Zahájení poskytování Služby KL04	Na základě Objednávky
Ukončení poskytování Služby KL04	Na základě Objednávky

2 REŽIM POSKYTOVÁNÍ SLUŽBY

Služba KL04 bude poskytována v režimu dle popisu v tabulce:

Režim poskytování Služby KL04	Doba poskytování Služby KL04
Standardní provozní doba	V pracovní dny (5x8) 8–16 h

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 VSTUPY

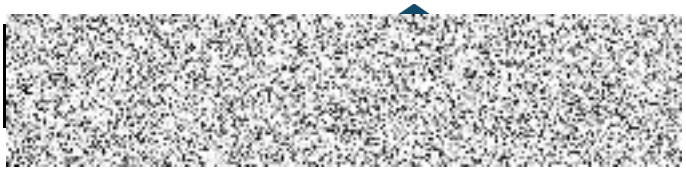
Vstupy dodané Objednatelem pro Službu KL04 jsou:

- 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 KL04 jsou:

- Poskytování Služby KL04;
- 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 KL04 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 KL04, 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 KL04 – Část 1 a Část 2

Služba KL04 je služba postavená na týmu odborníků pokrývajícím všechny potřebné kompetence a znalosti se zajištěnou zastupitelností.

Služba KL04 je určena jako odborná administrativní podpora v oblasti informační a kybernetické bezpečnosti pro Objednatele. Služba KL04 zajišťuje podporu vedení a správy systému řízení bezpečnosti informací (dále také „**SŘBI**"). Služba KL04 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 pro jednotlivé bezpečnostní role Objednavatele (např. manažer KB, architekt KB, auditor KB a další – bude určeno na základě Vstupní analýzy).

5 POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL04

Služba KL04 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 KL04 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 500 uživatelů, s tím, že přesný limit počtu uživatelů bude vždy obsažen v Objednávce k dané Službě dle tohoto Katalogového listu, a nastavení Nástroje dle prostředí Objednatele.

Dokumentem, pro potřeby Služby KL04, 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:

- vložením souboru dokumentu v digitální formě do modulu,
- 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 KL04 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 KL04 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 KL04. 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 KL04.

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 KL04. 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 KL04 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 KL04;
- Režim poskytování Služby KL04;
- Popis rozsahu Služby KL04;
- Provozovaná prostředí;
- Aktivity Služby KL04;
- Řízení provozu Služby KL04;
- Návrh na nápravná opatření a doporučení.

6 SLA PARAMETRY

Poskytovatel je povinen poskytovat Službu KL04 dle Smlouvy v rozsahu definovaném objednávkou, a to v níže uvedených parametrech.

Ovlivnění chodu všech částí Služby KL04 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 KL04.

6.1 POŽADOVANÁ MĚSÍČNÍ DOSTUPNOSTČÁSTI 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 KL04 – 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 KL04 – Část 1 a Část 2 ve výše definovaném rozsahu do okamžiku obnovení poskytování. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti Služby KL04 – 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 KL04 – Zpracování zprávy o stavu Služby KL04 dle tohoto katalogového listu určené Objednateli (předávána v měsíčním intervalu) - neovlivňuje dostupnost a kvalitu poskytované Služby KL04 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:

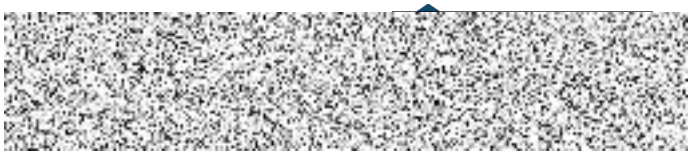
$$D = 100 * \frac{T-N}{T}$$

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 KL04.



6.1.2 Požadované lhůty pro obnovení Služby KL04 – 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 KL04 – Části 1 a Část 2

Kategorizace provozních incidentů	
Incident kategorie A	Služba KL04 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 KL04, 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 KL04

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 při přijetí Poskytovatelem vyhodnoceny a o celkové době pro vyřešení takových 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

Název Služby	Kompetenční centrum kybernetické bezpečnosti	
SLA parametry		
Část Služby	**Maximální doba reakce na požadavek Objednatele**	**Doba vyřešení požadavku**
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

Při přijetí požadavku dává Poskytovatel základní zpětnou vazbu.

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.

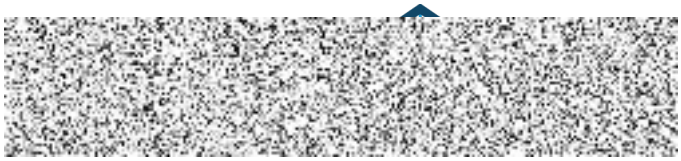
Maximální doba pro vyřešení požadavku v oblasti Část 1 – Administrace v Nástroji pro podporu řízení SŘBI a Část 2 – Administrativní podpora v oblasti Ochrany osobních údajů dle ZoKB platí v případě, že je z požadavku zřejmé, co Objednatel požaduje a že dodal úplné podklady pro vyřešení požadavku. V opačném 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 KL04 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 KL04 soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL04 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 KL04 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. Zahájení mimořádné odstávky může proběhnout pouze po odsouhlasení. Doba odstávky, která byla předem řádně ohlášena, se nezapočítává do nedostupnosti Služby KL04. Ovlivnění chodu Služby KL04 ze strany Objednatele se nezapočítává do nedostupnosti Služby KL04.



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 KL04 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 KL04 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 avýběru 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 KL04, 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 KL04 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 KL04;

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 KL04.

Hlášení poruchy Služby KL04 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 se Smlouvou a na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy a následné Realizace ověření provozu pro následné poskytování Služby KL04 – Administrace v Nástroji pro podporu řízení SŘBI.

Vstupní analýza bude použita pro návrh testovacího provozu, který bude ověřen při Realizaci ověření provozu, kde budou nastavena a ověřena technická řešení a procesy a budou stanovena množství jednotek pro zajištění řádného poskytování Služby KL04 – Administrace v Nástroji pro podporu řízení SŘBI.

Výsledná cena Služby KL04 – Administrace v Nástroji pro podporu řízení SŘBI se stanoví jako součin množství požadovaných jednotek a jejich jednotkové ceny uvedené ve Smlouvě.

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 KL04, 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 KL04, 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 KL04 dle kapitoly 3.2. Tyto služby mohou být realizovány na základě samostatné objednávky dílčích částí Služby KL04 a KL05 (Konzultace v oblasti informační a kybernetické bezpečnosti).

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.

9.2 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 zpracovaná Poskytovatelem a předaná Objednateli jako výstup na základě samostatné objednávky, 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.

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 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).

Výraz	Popis
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.

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 a poskytnutí rozvojových činností v oblasti syslog serverů. Vykonávání činností probíhá na základě požadavku Objednatele. 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 podpůrné činnosti plnění povinnosti bezpečnostní role vycházející ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) na straně Objednatele, pokud Objednatel nepožaduje výslovně plnění této role dle Zákona;
- 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 podpůrné činnosti plnění povinnosti bezpečnostní role vycházející ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) na straně Objednatele, pokud Objednatel nepožaduje výslovně plnění této role dle Zákona;
- 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 SPRÁVCE ZRANITELNOSTÍ

Správce zranitelností je osoba, která:

- zajišťuje provádění adhoc 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.

5.9 SPRÁVCE IDENTIT

- Správce identit je osoba, která:implementuje, spravuje a rozvíjí nástroje pro správu a řízení identit;
- školí uživatele v nástrojích pro správu a řízení identit;
- vytváří a aktualizuje provozní dokumentaci ke správě a řízení identit;
- provádí kontrolu nastavení nástrojů pro správu a řízení identit;
- spolupracuje na analýze, sběru, dekompozici a syntéze získaných informací a na návrhu implementace služby správa privilegovaných účtů;
- účastní se jednání s pracovníky Objednatele;
- zpracovává připomínky a návrhy k dokumentům předkládaným Objednatelem;
- vykonává metodickou a konzultační činnost v oblasti správa privilegovaných účtů.

5.10 ADMINISTRÁTOR UNIX

Administrátor UNIX je osoba, která:

- 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;
- provádí upgrady Syslog NG a migraci do jiného prostředí, jiný OS;
- aktualizuje Dokumentaci a iniciuje projednání možných dalších směrů rozvoje použité Syslog NG a syslog serverů;
- provádí rekonfiguraci způsobu ukládání logů;
- vyvíjí a nastavuje čtení logů ze zdrojů, které neumožňuje odesílání logů do Syslog NG (nutnou podmínkou je umožnit Poskytovateli přístup na tyto zdroje ze strany Objednatele);
- připravuje podklady pro reporting dodržování SLA a pro technický rozvoj.

5.11 ADMINISTRÁTOR APLIKACE

Administrátor aplikace je osoba, která:

- 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

5.12 IT ANALYTIK / IT ARCHITEKT

IT Analytik / IT Architekt je osoba, která:

- Analyzuje potřeby a požadavky na ICT infrastrukturu a navrhuje technický způsob jejich řešení s využitím portfolia standardních HW/SW komponent provozně adoptovaných technologických znalostí a zavedených sdílených služeb pro dosažení efektivity a nákladové optimalizace při jejich realizaci i v následném provozu;
- aktualizuje Dokumentaci a iniciuje projednání možných dalších směrů rozvoje použité Syslog NG a syslog serverů;
- zpracovává technické projekty a vytváří podklady pro jejich implementaci;
- navrhuje směry dalšího rozvoje a využití nových technologií a poskytuje odborné konzultace v oblasti ICT technologií a technické architektury.

5.13 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 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 Služby KL05 v rámci dané role v předmětném kalendářním měsíci na základě dané Objednávky.

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

Poskytnutí jednotlivých rolí je realizováno zejména pracovníky SPCSS a jednotlivé činnosti jsou realizovány prostřednictvím odpovídajících rolí dle kapitoly 5.

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.
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.

Výraz	Popis
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 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.

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 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
☒	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
  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**
Část 2 – Vulnerability management	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.

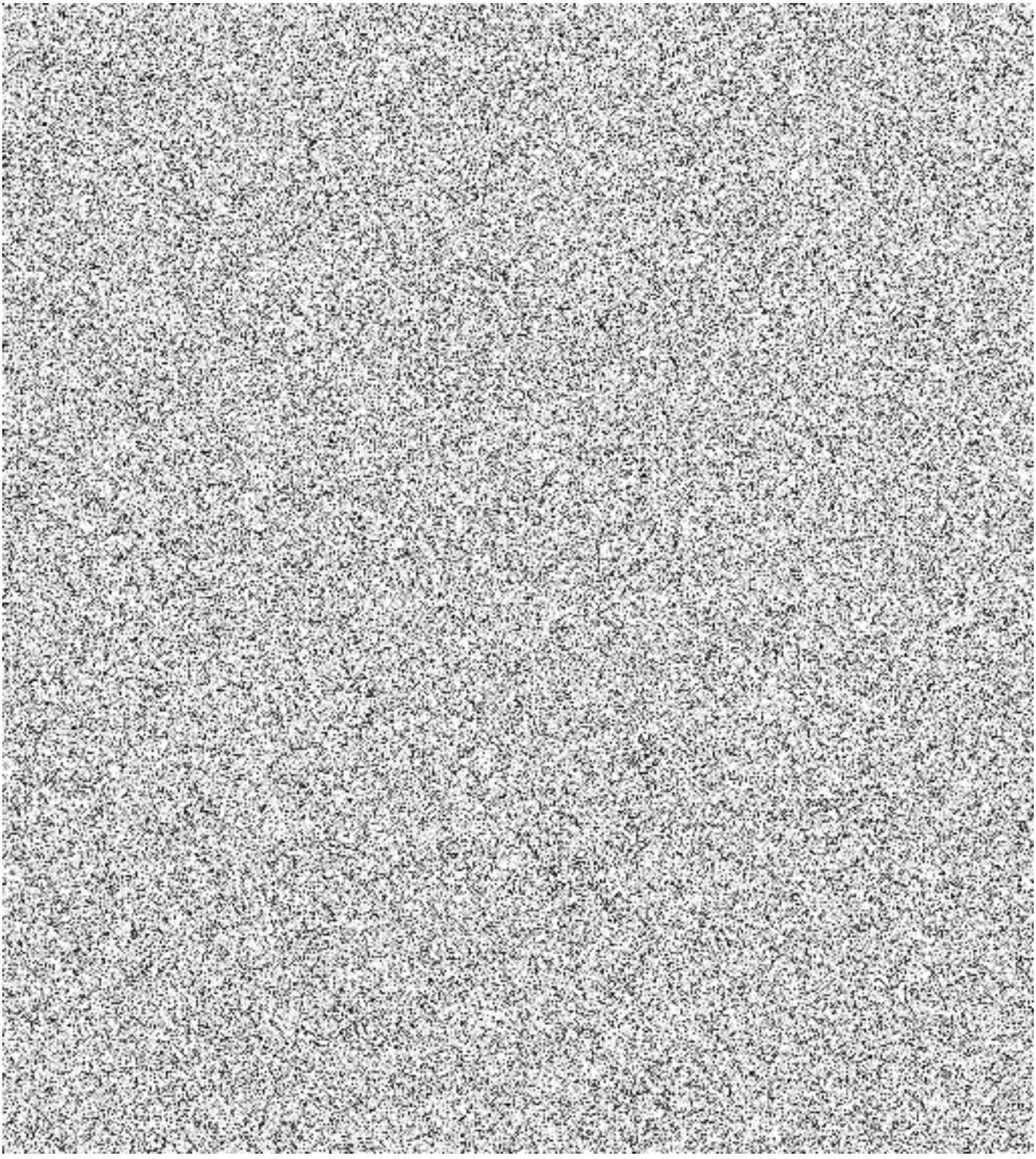
Maximální doba pro vyřešení požadavku v oblasti Část 1 – Ad-hoc sken platí v případě, že je z požadavku zřejmé, co Objednatel požaduje a že dodal úplné podklady pro vyřešení požadavku. V opačném případě se doba vyřešení požadavku prodlužuje o dobu potřebnou k vyjasnění požadavku nebo doplnění podkladů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

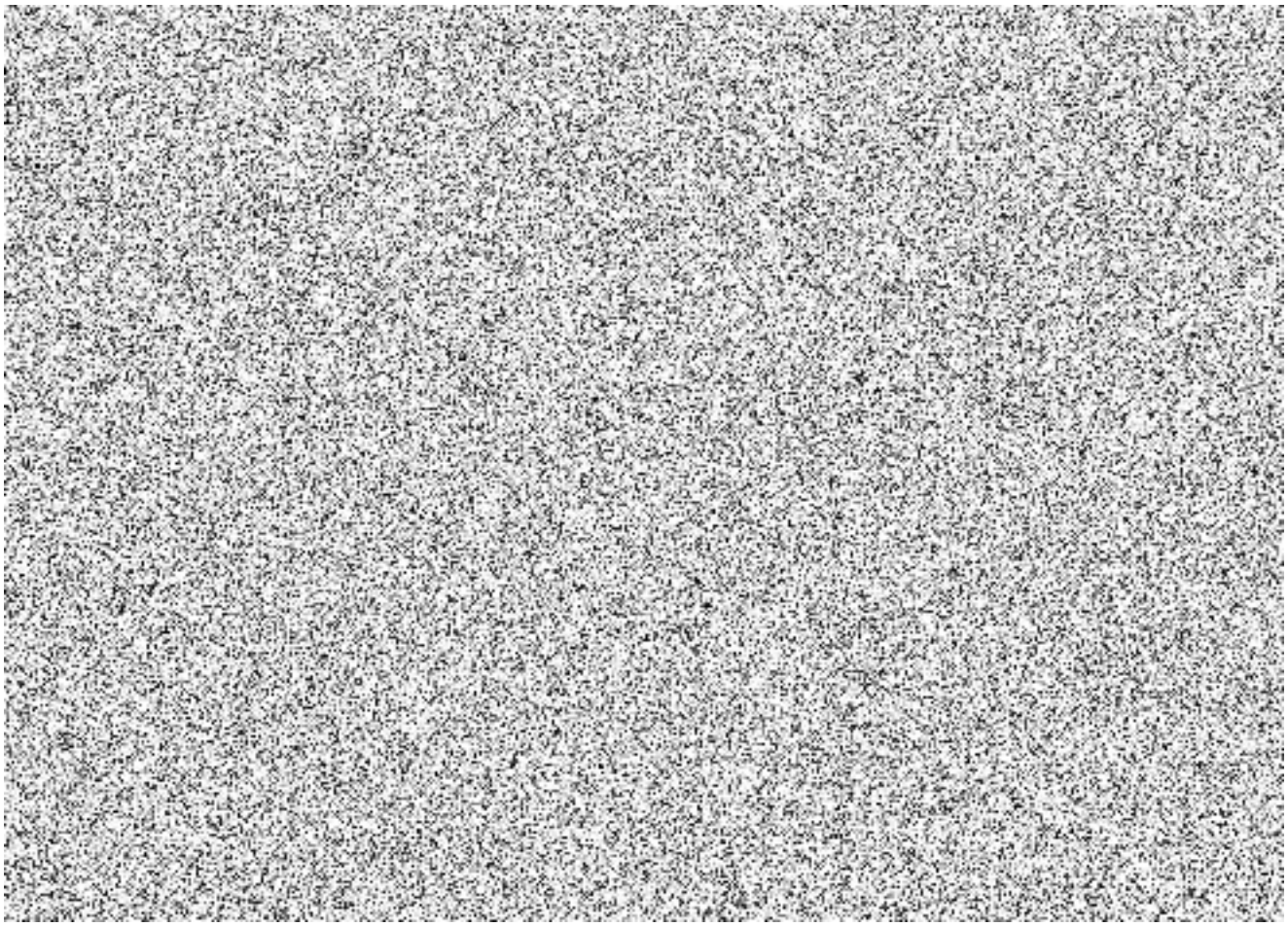
6.4 PLÁNOVANÉ ODSTÁVKY

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

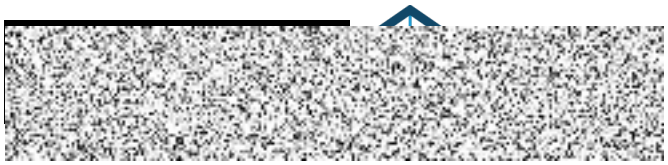




8 SOUČINNOST PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY

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 se Smlouvou a na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Dodavatelem, a to formou a za podmínek Vstupní analýzy pro následné poskytování Služby KL06.

V rámci Vstupní analýza bude stanoveno množství jednotek pro zajištění řádného poskytování Služby KL06. Výsledná cena Služby KL06 se stanoví jako součin množství požadovaných jednotek a jejich jednotkové ceny uvedené dle 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 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.

Výraz	Popis
NIST	The National Institute of Standards and Technology

KATALOGOVÝ LIST č. 07	
Název služby	**Správa syslog serverů**

1 OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Správa syslog serverů (dále jen **„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
Část 1: Správa serverů	
Běžná provozní doba	Pracovní dny 6:00 – 20:00 hod
Rozšířená provozní doba	Pracovní dny 20:00 – 6:00 hod a mimo pracovní dny 24 hodin denně

3 VSTUPY A VÝSTUPY SLUŽBY

3.1 VSTUPY

Vstupy dodané Objednatelem pro Službu KL07 jsou:

- relevantní dokumenty Objednatele (technická provozní a bezpečnostní dokumentace);
- politika pro systém řízení bezpečnosti GFŘ;
- Registr rizik GFŘ a jejich protiopatření.

3.2 VÝSTUPY

Výstupy Služby KL07 jsou:

- Poskytování Služby KL07;
- měsíční zpráva o stavu služby dle tohoto katalogového listu.

4 POPIS ROZSAHU SLUŽBY

Služba KL07 zahrnuje správu operačního systému serverů dedikovaných pro provoz syslog serverů a na nich provozovaných Syslog NG serverů .

Služba KL07 je určena k zajištění správy operačních systémů a na nich provozovaných Syslog NG serverů, blíže popsáno v kapitole 5.1.

Část 1 (ID=01) - Správa serverů (nedílná součást KL07, poskytováno vždy)

5 POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL07

5.1 SPRÁVA SERVERŮ

Součástí služby Správa serverů je převzetí správy operačních systémů a na nich provozovaných Syslog NG serverů týmem Poskytovatele. Dále se Poskytovatel zavazuje dodržovat relevantní ustanovení politiky GFŘ a VoKB. V následujících bodech jsou jednotlivé činnosti podrobněji specifikovány. Služba je Poskytovatelem zajišťována jako paušální plnění.

Správa operačních systémů serverů dedikovaných pro provoz dvou syslog serverů a na nich provozovaných Syslog NG serverů (servery dc1log1, dc2log1) obsahuje následující činnosti:

- správu operačního systému AIX včetně jeho dohledu a patchování;
- správu produktu Syslog NG;
- přidání/odebrání logsources;
- aplikace patchů;
- řešení chybových stavů a součinnost při řešení problémů;
- řešení zranitelností
- administrace rozhraní Syslog NG, konfigurace přeposílání logů;
- administrace TSM klienta pro potřeby zálohování;
- dohled běhu standardního syslog (součást AIX);
- aktualizace Dokumentace
- dohled běhu produktu Syslog NG;
- dohled nad platností certifikátů pro Syslog NG, měsíc před vypršením zaslání žádosti na Objednatele o obnovení certifikátů;
- dohled nad kapacitami diskových prostorů;
- předání logu/ů syslog a Syslog NG serverů do sdíleného úložiště Objednatele, na základě požadavku určených osob Objednatele (datum, server, typ logu) v aplikaci Service Desk Poskytovatele (servicedesk.spcss.cz), dále jen „Service Desk", analýza obsahu logu není součástí Služby;
- pro případné testování prostředí před rekonfigurací a aplikaci patchů Syslog NG a potřebných restartů bude využit server dc2log1, kam logují neostrá prostředí.

Správa serverů neobsahuje

- garanci doručení logů na Syslog NG server, správu infrastruktury, správu odesílajících zdrojů;
- pořízení nových certifikátů, nové certifikáty budou předávány elektronicky (vzdáleným přístupem);
- správu HW a virtualizační platformy;
- rozvojové práce.

5.2 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;
- Plánované a schválené mimořádné odstávky ve vykazovaném období;
- Statistika servisních hlášení;

- Statistika závad dle kategorií;
- Statistika servisních hlášení s překročením garantované doby reakce;
- Tabulka s garantovanou roční dostupností do konce vykazovaného období;
- Cena služby KL07
- Splnění kvalitativních parametrů poskytování Služby KL07.

6 SLA PARAMETRY

Poskytovatel je povinen poskytovat Službu KL07 dle Smlouvy v souladu s jednotlivými níže uvedenými kvalitativními parametry Služby pro její jednotlivé části.

Ovlivnění chodu všech částí Služby KL07 ze strany Objednatele z důvodů mimo působnost Poskytovatele se nezapočítává do nedostupnosti žádné z částí Služby KL07.

6.1 ROČNÍ DOSTUPNOST SLUŽBY

Požadavek na roční dostupnost Služby podle tohoto Katalogového listu je uveden v následující tabulce:

Roční dostupnost			
v běžné provozní době		**v rozšířené provozní době**	
v %	**výpadek v hodinách**	**v %**	**výpadek v hodinách**
99,5	17,64	98,0	105, 12

6.2 REAKČNÍ DOBY SLUŽBY

Doba reakce je počítána od zaevidování odpovídajícího hlášení do aplikace Service Desk (servicedesk.spcss.cz).

Název Služby	**Maximální doba zahájení řešení incidentu v běžné provozní době v hodinách**		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Správa serverů	1	1	3

Poskytovatel je povinen Incident vyřešit v co nejkratším možném termínu, případně v termínu dle dohody s Objednatelem. Incident se považuje za vyřešený jeho úplným vyřešením nedohodnou-li se smluvní strany jinak.

Tabulka: Kategorizace provozních incidentů:

Incident kategorie A	Službu není možno využívat, žádné logy nejsou přijímány a zpracovávány. Tento stav kritickým způsobem omezuje běžný provoz.
Incident kategorie B	Službu je možno využívat v omezeném rozsahu, logy jsou přijímány a zpracovávány pouze z některých zdrojů.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

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.

6.2.1 Definice měření dostupnosti

Dostupnost Službyje definovaná jako splnění všech následujících podmínek:

- OS syslog NG serverů je dostupný pro provoz aplikace;
- procesy aplikace syslog NG fungují, tj. aplikace je připravena přijímat data z odesílajících klientů (s výjimkou případů nedostatečnosti HW prostředků).

Za nahlášení nedostupnosti Služby se považuje okamžik založení odpovídajícího hlášení Objednatelem v aplikaci Service Desk nebo založení na základě automatického hlášení incidentu dohledovým systémem Poskytovatele. Pro výpočet nedostupnosti jsou časy zaokrouhleny na celé minuty. Do doby nedostupnosti se započítávají všechny doby incidentů kategorie A včetně neplánovaných odstávek. Pokud byl incident způsoben prokazatelně mimo zodpovědnost Poskytovatele, do doby nedostupnosti se nezapočítává. Do doby nedostupnosti se také nezapočítává doba plánovaných odstávek.

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 a mimořádné odstávky.

6.2.2 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:

- k nedostupnosti nebo závadě dojde ze strany Objednatele mimo působnost Poskytovatele
- k nedostupnosti nebo závadě dojde mimo infrastrukturu Poskytovatele (zejména v infrastruktuře GFŘ);
- Poskytovatel není informován o změnách, které mohou mít vliv na příjem logů ze zdrojů logů a na přenosovou infrastrukturu;

- vyskytnou se okolnosti, které představují událost vyšší

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 ohlašovány a realizovány i mimo tato servisní okna. Doba odstávky, která byla předem řádně ohlášena se nezapočítává do nedostupnosti Služby KL07. Za ohlášení se považuje informování určených osob Objednatele e-mailem, a to minimálně 24 h před zahájením mimořádné odstávky.

7 PRINCIP STANOVENÍ CENY

Cena bude stanovena v souladu s Přílohou č. 13 Smlouvy a na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy pro následné poskytování Služby KL07.

7.1 MĚSÍČNÍ CENA ZA SLUŽBU

Objednatel hradí měsíční cenu za Službu dle tohoto odstavce měsíčně, a to vždy zpětně za každý kalendářní měsíc poskytování Služby, poprvé však v měsíci, ve kterém bylo započato s poskytováním Služby dle čl. 1 tohoto Katalogového listu, a to vždy na základě faktury vystavené Poskytovatelem. Smluvní strany se dohodly, že v případě, že Služba nebude poskytována po celý kalendářní měsíc, (tj. v případě, když bude s poskytováním Služby započato v průběhu kalendářního měsíce, případně bude poskytování Služby ukončeno v průběhu kalendářního měsíce), se měsíční cena za Službu dle tohoto odstavce poměrně krátí, a to s přesností na celé dny poskytování Služby a Poskytovateli náleží alikvotní část měsíční ceny za Službu dle tohoto odstavce.

8 SOUČINNOST PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY

Za účelem zajištění Služby poskytne Objednatel nezbytnou součinnost při:

- předání seznamu určených osob pro plnění Služby Poskytovateli do 5 dnů od zahájení poskytování Služby. Objednatel je povinen každou změnu určených osob prokazatelně ohlásit Poskytovateli. Požadavky v rámci Služby jsou Objednatelem zadávány pomocí Service Desku dle seznamu určených osob;
- zajištění nepřetržitého spojení na cílové systémy, tj. prostup z perimetru Poskytovatele do perimetru Objednatele formou nastavení pravidel na Firewallu Objednatele/ site-to-site VPN;
- stanovení termínů odstávek;
- předání přístupové informace (účet root);
- zajištění podpory produktu Syslog NG a zprostředkování této podpory pro Poskytovatele;
- využívání Service Desku za účelem zadání a řešení provozních požadavků a incidentů;
- provozním dohledu HW, virtualizačního prostředí, zálohování a automatizovaného předávání informací o stavu;
- předání aktuální technické provozní a bezpečnostní dokumentace pro ověření realizace provozu Poskytovatelem;
- přístupu na HMC (ovládací prvek Power serverů) s právy ovládat dotyčné AIXy (restartovat je z úrovně HW, zpřístupnění HW konzole, pokud AIX neodpovídá);
- obnově certifikátů;
- zajištění veškerých nezbytných licencí;
- přidělení přístupu pro zápis a síťového spojení do sdíleného úložiště Objednatele při předání logů, dle požadavku Objednatele.

Poskytovatel poskytne nezbytnou součinnost při:

- ukončení Služby, včetně předání aktuální veškeré Dokumentace Objednateli;
- kontrole objednatele;
- auditu objednatele.

9 PŘEDPOKLADY PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY

Bude naplněna požadovaná součinnost z čl. 8.

Komunikačním kanálem pro hlášení incidentů a požadavků určenými pracovníky Objednatele je Service Desk. Service Desk je dostupný v režimu 24x7.

ServiceDesk je pracoviště Poskytovatele přijímající servisní hlášení od určených osob Objednatele přes webové rozhraní Service Desku, telefonicky nebo e-mailem.

- 

Service Desk je standardním nástrojem a službou SPCSS pro poskytování podpory a řízení provozních procesů. Service Desk je využíván jako prostředek formalizovaného způsobu komunikace s uživateli a pracovníky podpory provozu GFŘ i třetích stran.

Service Desk bude využíván pro předávání informací o provozních incidentech a požadavcích a sledování postupu jejich řešení. Řešitelé incidentů a požadavků budou pracovat přímo v prostředí Service Desk. SPCSS je odpovědný za včasný záznam postupu řešení incidentů (v rozsahu jeho odpovědnosti) v Service Desku, v úrovni detailu dostatečné pro spolupráci ostatních účastníků provozu na jejich řešení a pro zpětný audit příčin incidentů a způsobu řešení.

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

10 POUŽITÉ VÝRAZY

Výraz	Popis
SPCSS	Státní pokladna Centrum sdílených služeb, s. p.
GFŘ	Generální finanční ředitelství
MD	Man Day – člověkoden, pracovní den v rozsahu 8 pracovních hodin
AIX	Advanced Interactive eXecutive je název proprietárního UNIXového operačního systému firmy IBM.
Syslog NG	Aplikace, která shromažďuje a ukládá systémové logy ze satelitních systémů.
Syslog server	V tomto případě operační systém (AIX), na kterém je provozována aplikace Syslog NG. Součástí je i systémová komponenta AIXu syslog.

ŘÍZENÍ POSKYTOVÁNÍ SLUŽBY

Tato příloha popisuje metodiku a procesy řízení Služeb ve spolupráci Poskytovatele (SPCSS) a Objednatele (GFŘ).

1. ŘÍDÍCÍ STRUKTURY POSKYTOVÁNÍ SLUŽBY

1.1 Řídicí komise

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

1.2 Manažeři Služeb a TPP

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

Manažeři Služeb za GFŘ a SPCSS jsou Oprávněné osoby dle Smlouvy. Manažeři Služeb GFŘ a SPCSS zodpovídají za řádné plnění povinností svých Smluvních stran v rámci poskytování Služby. Připravují podklady k rozhodování ŘKO.

Manažer služeb SPCSS zpracovává 1x měsíčně Zprávu dle Smlouvy a předkládá ji Manažerovi služeb za GFŘ k akceptaci.

Jednání Status:

- pravidelné jednání, periodicita je dána dohodou obou Smluvních stran a alespoň 1x měsíčně;
- na jednání je řešen stav připravovaných a poskytovaných Služeb;
- je složen ze zástupců SPCSS, GFŘ a případně i dalších třetích stran ve smluvním vztahu s GFŘ nebo SPCSS;
- řeší aktuální problémy, jak ve fázi přípravy Služeb, tak ve fázi poskytování Služeb;
- identifikuje možná rizika;
- zajišťuje mitigaci rizik;
- projednává návrhy na optimalizaci a změnu.

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

- je složen ze zástupců SPCSS, GFŘ a případně i dalších třetích stran ve smluvním vztahu s GFŘ nebo SPCSS;
- řeší aktuální problémy, jak ve fázi přípravy Služeb, tak ve fázi poskytování Služeb;
- identifikuje možná rizika;
- řídí a monitoruje kvalitu poskytování Služeb s ohledem na identifikované problémy a rizika. Analyzuje a posuzuje rizika. Projednává a schvaluje návrhy na mitigaci identifikovaných rizik s cílem minimalizace rizika a jeho dopadů;
- zajišťuje mitigaci rizik;
- identifikuje a projednává změny předmětu Smlouvy, termínů, ceny nebo kvality plnění. Analyzuje dopady změn na Služby a předkládá návrhy ŘKO;
- projednává a předkládá návrhy na optimalizaci a změnu.

Před zahájením poskytování Služby Oprávněné osoby Smluvních stran sestaví a vzájemně odsouhlasí seznam kontaktních osob pro předávání a řízení incidentů, požadavků a součinností dle jednotlivých katalogových listů. V průběhu poskytování Služby může Oprávněná osoba každé Smluvní strany změnit kontaktní informace své strany se souhlasem Oprávněné osoby druhé strany. Oprávněná osoba Poskytovatele se zavazuje vést aktuální seznam kontaktních a určených osob dle Přílohy č. 1 až č. 7 této Smlouvy.

2. ŘÍDICÍ DOKUMENTACE POSKYTOVÁNÍ SLUŽBY

Řídicí dokumentace poskytování Služby je uvedena v jednotlivých katalogových listech a obsahuje zejména:

- procesy řízení;
- specifické postupy při poskytování Služby;
- komunikační plán (pravidla komunikace, reporting);
- strukturu a nominace členů pracovních týmů.

Změny Řídicí dokumentace poskytování Služby mohou být iniciovány ŘKO, Manažerem služeb GFŘ nebo Manažerem služeb SPCSS.

Na úrovni TPP bude dále spravována sada řídicích dokumentů:

- registr úkolů a součinností;
- registr problémů a změn;
- registr provozních rizik;
- zprávy a reporty;
- zápisy z jednání.

3. NÁSTROJE ŘÍZENÍ POSKYTOVÁNÍ SLUŽBY

Pro řízení služby je určen Service Desk Poskytovatele. Service Desk je dostupný v režimu 24x7, a to přes:

- 

ServiceDesk je využíván pro předávání informací o incidentech, požadavcích a sledování postupu jejich řešení dle specifikace jednotlivých Služeb dle Přílohy č. 1 až č. 7 této Smlouvy.

Service Desk bude využíván pro předávání informací o incidentech a požadavcích a sledování postupu jejich řešení.

4. VYMEZENÍ ODPOVĚDNOSTÍ

Odpovědnosti a součinnosti SPCSS

Řízení součinností SPCSS probíhá prostřednictvím Service Desku v rámci jednotlivých procesů poskytování Služby v souladu s Přílohami č. 1 až 7 této Smlouvy nebo formou zápisů z jednání TPP.

Řešení všech incidentů, požadavků, problémů, rizik a změn (včetně součinností v rámci odpovídajících procesů), které souvisí s prevencí výskytu, opravou nebo řešením následků incidentů, aktualizací SW produktů, které jsou součástí Služeb, a souvisejících úprav nebo migrací dat, nebo jejichž příčina nebyla dosud jednoznačně určena mimo oblast odpovědnosti SPCSS, je součástí ceny Služeb. Všechny pravidelné a proaktivní činnosti, které jsou nezbytné pro poskytování Služeb bez výskytu incidentů v oblastech odpovědnosti SPCSS, jsou rovněž součástí ceny Služeb.

5. ŘÍZENÍ ZMĚN

Změny, které mají vliv na rozsah nebo funkcionalitu poskytovaných Služeb dle této Smlouvy, jsou realizovány formou Změnového řízení dle této Smlouvy.

6. ŘÍZENÍ PROBLÉMŮ

Problém je příčina jednoho nebo více incidentů. Příčina obvykle není známa v čase vytvoření záznamu o problému a proces řízení problémů je odpovědný za jeho další zkoumání.

Cílem řízení problémů není případným problémům či změnám v projektu zabránit, ale řešit je. Každý problém je třeba co nejdříve identifikovat, navrhnout řešení a řešení posoudit a schválit.

Problémy jsou průběžně identifikovány a řešeny v rámci jednání a úkolů TPP. SPCSS je povinen řešit problémy v rámci pracovní doby bez zbytečného odkladu, s ohledem na závažnost problému, určenou GFŘ. Do určení příčiny incidentu řeší SPCSS problémy přidělené GFŘ jako problémy v odpovědnosti SPCSS.

Pokud řešení problému vyžaduje změnu Služeb, postupuje se podle pravidel Změnového řízení a je vypracován Změnový požadavek.

Problémy, které výrazným způsobem negativně ovlivňují parametry Služeb, musí být s GFŘ řádně projednány, zdokumentovány a řízeny (např. v zápise z jednání TPP). Za toto projednání, zdokumentování a řízení odpovídá Manažer služeb SPCSS.

7. ŘÍZENÍ RIZIK

Rizika je třeba včas identifikovat, správně vyhodnotit, stanovit vhodná opatření, implementovat je a vyhodnotit účinnost opatření.

1. Zřízení a údržba registru rizik je součástí agendy TPP.
2. Riziko může identifikovat kdokoliv, oznámí ho manažerovi služeb nebo v rámci jednání TPP a TPP zaeviduje riziko do registru rizik, vyhodnotí jeho význam a navrhne opatření k minimalizaci dopadu rizika.
3. V případě, že TPP identifikuje rizika, která přesahují jeho kompetence, postoupí je neprodleně k projednání a schválení na ŘKO.
4. TPP určí vlastníka rizika, vlastník rizika odpovídá za implementaci zvoleného opatření.
5. TPP a vlastník rizika vyhodnotí účinnost opatření.
6. TPP min. 1x za rok nebo na základě informace o změně stavu evidovaného rizika reviduje registr rizik, a kromě aktualizace rizik zhodnotí účinnost přijatých opatření.
7. V případě, že riziko, resp. schválené opatření vyvolá změnu základních kritérií Služby, je vytvořen a zpracován Změnový požadavek – postupem popsaným v čl. VII. Změnové řízení Smlouvy.

V rámci identifikace rizik musí být určeny:

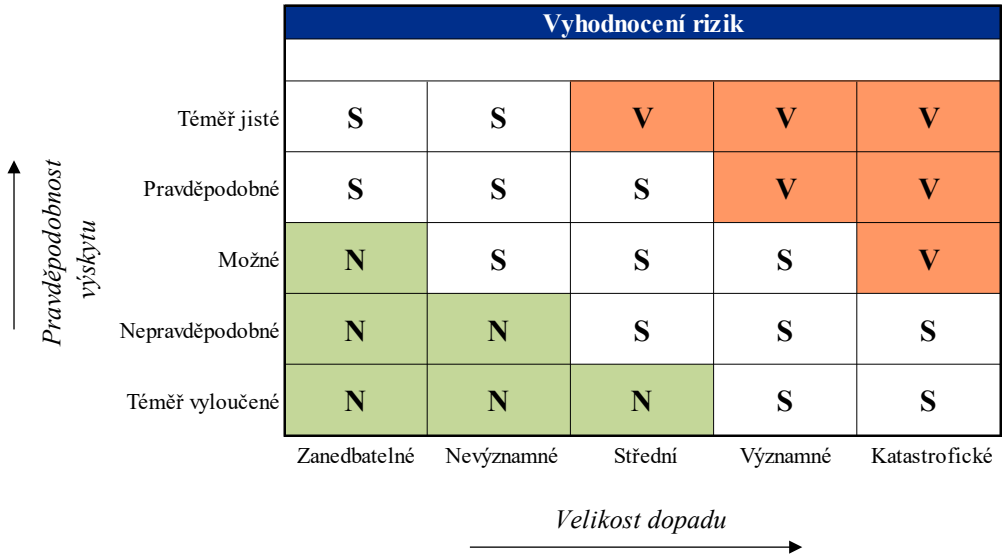
- příčina rizika (reálná událost nebo situace, která je důvodem vzniku rizika);
- riziko (událost, která může s určitou pravděpodobností nastat);
- dopad na kvalitu a parametry poskytované Služby.

Rizika jsou hodnocena z hledisek:

- pravděpodobnosti, že riziková situace nastane (stupeň 1-5);
- rozsahu dopadu v případě, že riziková událost nastane (stupeň 1-5);
- časového horizontu, ve kterém může daná riziková událost nastat.

Pravděpodobnost		**Dopad**	
1	Téměř vyloučené	1	Zanedbatelný
2	Nepravděpodobné	2	Nevýznamný
3	Možné	3	Střední
4	Pravděpodobné	4	Významný
5	Téměř jisté	5	Katastrofický

Součin hodnot pravděpodobnosti výskytu a dopadu určuje váhu rizika. Čím vyšší je hodnota součinu, tím je riziko významnější. Rizika se rozdělí na 3 kategorie podle jejich významu – nízký (N), střední (S), vysoký (V) pomocí následující matice hodnocení rizik:



8. ŘÍZENÍ KVALITY

Řízení kvality poskytování Služby probíhá v rámci jednání a úkolů řídicích orgánů a prostřednictvím pravidelných měsíčních Zpráv dle Smlouvy.

Řízení kvality probíhá zejména v oblastech:

- plnění SLA parametrů;
- dodržování procesů řízení incidentů a požadavků;
- prováděné pravidelné a proaktivní činnosti a servisní zásahy;
- dodržování procesu řízení změn a konfigurací;
- plánování a řízení změn většího rozsahu, včetně testování a nasazení do produktivního provozu;
- systematické vyhodnocování stavu otevřených problémů a rizik.

Měsíční **Zpráva o úrovni a rozsahu poskytovaných Služeb** (dále jen „Zpráva") dle této Smlouvy bude obsahovat informace o reálném plnění výkonnostních a SLA parametrů a bude hodnocena podle jejich souladu s hodnotami uvedenými Přílohách č. 1 až č. 7 této Smlouvy.

Konečné vypořádání závažného incidentu ve formě Incident reportu je vždy součástí příslušné měsíční Zprávy.

9. KOMUNIKACE

Veškerá komunikace v rámci poskytování Služby probíhá v češtině.

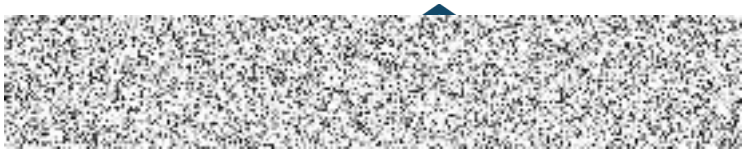
Základním komunikačním kanálem je e-mail. Všechny důležité předávané informace prostřednictvím e-mailu budou zasílány v kopii vždy oprávněným osobám.

Vedlejším komunikačním kanálem je telefon nebo osobní jednání. Všechny významnější dohody provedené prostřednictvím telefonu musí být dodatečně potvrzeny e-mailem nebo písemně formou zápisu z jednání.

Z jednání TPP a ŘKO se pořizuje zápis a po schválení zápisu je tento distribuován všem účastníkům jednání a dalším určeným osobám.

Frekvence jednání týmů:

- TPP: Základní interval jednání TPP je 1x měsíčně. Tento interval může být upraven dohodou mezi manažery služeb obou Smluvních stran. Každý z manažerů služeb je oprávněn iniciovat mimořádné jednání TPP v případě potřeby – např. při identifikaci nového rizika;
- ŘKO: Základní interval jednání ŘKO je 1x ročně. Toto jednání může proběhnout i korespondenčně, schválením předem připraveného textu zápisu z jednání. Kromě toho může být jednání ŘKO svoláno dle potřeby identifikované manažery služeb za účelem rozhodnutí o Změnovém požadavku, uplatnění smluvní sankce nebo eskalaci neshody na úrovni TPP.

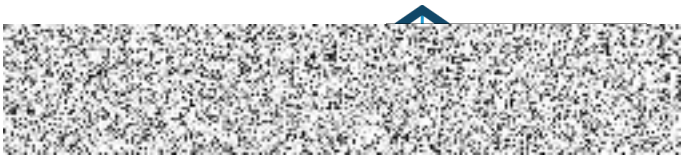


Eskalační úrovně:

- Případné neshody v rámci poskytování Služeb jsou řešeny na úrovni TPP.
- Případné neshody na úrovni TPP jsou řešeny v rámci jednání ŘKO.

10.ŘÍZENÍ SOUČINNOSTÍ

V případě potřebné součinnosti obou Smluvních stran, případně i jejich dodavatelů (třetích stran), jedna ze Smluvních stran požádá druhou Smluvní stranu o součinnost. Řízení součinností v rámci jednotlivých poskytovaných Služeb probíhá primárně prostřednictvím ServiceDesku, případně prostřednictvím e-mailu. Žádosti o ostatní součinnosti jsou identifikovány a schvalovány v rámci TPP nebo vyžádány manažerem služeb jedné Smluvní strany prostřednictvím šifrovaného e-mailu a potvrzeny manažerem služeb druhé Smluvní strany.



NABÍDKA

Rámcová smlouva o poskytování služeb v oblasti informační a kybernetické bezpečnosti (dále jen „Smlouva")	Evidenční číslo Objednatele - 24/7700/0034u Evidenční číslo Poskytovatele - SML2024019
Identifikační údaje Objednatele	**Identifikační údaje Poskytovatele**
Česká republika – Generální finanční ředitelství se sídlem: Lazarská 15/7, 117 22 Praha 1 za niž jedná: generální ředitelka IČO: 72080043 DIČ: CZ72080043 Bank. spojení: číslo účtu: ID DS: p9iwj4f	**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: 1. zástupcem generálního ředitele IČO: 036 30 919 DIČ: CZ03630919 Bank. spojení: číslo účtu: 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 nebo pododst. 2.4.2 nebo pododst. 2.4.3 nebo pododst.2.4.4 (v rozsahu Administrace SŘBI) nebo pododst. 2.4.6 Smlouvy nebo pododst. 2.4.7 Smlouvy]
Celková cena za nabízený počet člověkodnů	[bude doplněno v případě Nabídky na Službu dle čl. II odst. 2.4 poddost. 2.4.4 (v rozsahu Metodické podpory) nebo pododst. 2.4.5 Smlouvy]
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]
Harmonogram a návrh postupu plnění Exit plánu	[bude odstraněno, pokud není požadováno]

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]

Rámcová smlouva o poskytování služeb v oblasti informační a kybernetické bezpečnosti

Příloha č. 10: Vzor Objednávky

OBJEDNÁVKA

Rámcová smlouva o poskytování služeb v oblasti informační a kybernetické bezpečnosti (dále jen „Smlouva")	Evidenční číslo Objednatele - 24/7700/0034 Evidenční číslo Poskytovatele - SML2024019
Identifikační údaje Objednatele	**Identifikační údaje Poskytovatele**
Česká republika – Generální finanční ředitelství se sídlem: Lazarská 15/7, 117 22 Praha 1 za niž jedná: generální ředitelka IČO: 72080043 DIČ: CZ72080043 Bank. spojení: číslo účtu: ID DS: p9iwj4f	**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: 1. zástupcem generálního ředitele IČO: 036 30 919 DIČ: CZ03630919 Bank. spojení: číslo účtu: ID DS: ag5uunk
Objednávka číslo	[bude doplněno]
Preambule	[bude doplněno]
Název, specifikace a rozsah Služby	[bude doplněno]
Vstupy pro Službu dle čl. IV odst. 4.1 Smlouvy	[bude doplněno]
Požadavky na součinnost Objednatele	[bude doplněno]
Požadavky na součinnost třetích stran	[bude doplněno]
Harmonogram realizace Služby	[bude odstraněno, pokud není 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 dle Nabídky	[bude odstraněno, pokud není relevantní v rámci nabízené Služby]
Akceptační kritéria	[bude odstraněno, pokud nejsou relevantní v rámci nabízené Služby]
Bezpečnostní podmínky	[bude odstraněno, nejsou-li požadovány]
Místo plnění	[bude doplněno]
Harmonogram a návrh postupu plnění Exit plánu	[bude odstraněno, pokud není požadováno]

Služba	Počet jednotek za měsíc	Počet měsíců poskytování Služby dle harmonogramu	Cena celkem v Kč bez DPH	Cena celkem V Kč včetně DPH

[bude doplněno]	[bude doplněno]	[bude doplněno]	[bude doplněno]	[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]		

ZÁZNAM O POSKYTNUTÍ SLUŽEB

Rámcová smlouva o poskytování služeb v oblasti informační a kybernetické bezpečnosti (dále jen „Smlouva")	Evidenční číslo Objednatele - 24/7700/0034 Evidenční číslo Poskytovatele – SML2024019
Vykazované období	[bude doplněno]
Identifikační údaje Objednatele	**Identifikační údaje Poskytovatele**
Česká republika – Generální finanční ředitelství se sídlem: Lazarská 15/7, 117 22 Praha 1 za niž jedná: generální ředitelka IČO: 72080043 DIČ: CZ72080043 Bank. spojení: [redacted] číslo účtu: [redacted] ID DS: p9iwj4f	**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] 1. zástupcem generálního ředitele IČO: 036 30 919 DIČ: CZ03630919 Bank. spojení: [redacted] číslo účtu: ID DS: ag5uunk

Obě Smluvní strany potvrzují, že v uvedeném období byly v souladu se Smlouvou 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
[bude doplněno]	[bude doplněno]	[bude doplněno]	[bude doplněno]
Celkem			

Detailní přehled poskytnutých Služeb bude uveden v měsíční Zprávě o úrovni a rozsahu poskytovaných Služeb.

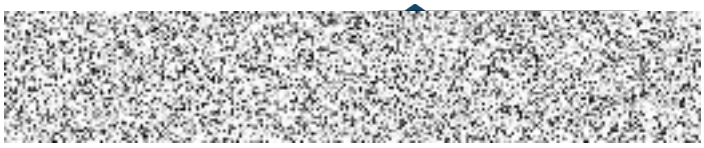
Schvalovací doložka

Jméno a příjmení	Organizace	Datum a podpis
[bude doplněno]	Objednatel	[elektronický podpis včetně data podpisu]
[bude doplněno]	Poskytovatel	[elektronický podpis včetně data podpisu]

ZPRÁVA
o úrovni a rozsahu poskytovaných Služeb

Rámcová smlouva o poskytování služeb v oblasti informační a kybernetické bezpečnosti (dále jen „Smlouva")	Evidenční číslo Objednatele - 24/7700/0034 Evidenční číslo Poskytovatele – SML2024019
Vykazované období	[bude doplněno]
Identifikační údaje Objednatele	**Identifikační údaje Poskytovatele**
Česká republika – Generální finanční ředitelství se sídlem: Lazarská 15/7, 117 22 Praha 1 za niž jedná: generální ředitelka IČO: 72080043 DIČ: CZ72080043 Bank. spojení: číslo účtu: ID DS: p9iwj4f	**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: 1. zástupcem generálního ředitele IČO: 036 30 919 DIČ: CZ03630919 Bank. spojení: číslo účtu: ID DS: ag5uunk

1) Období a režim poskytování Služeb
[bude doplněno]
2) Rozsah poskytovaných Služeb
[bude doplněno]
3) Řešení závad
[bude doplněno]
4) Servisní zásahy a provozní změny
[bude doplněno]
5) Dostupnost Služeb
[bude doplněno]
6) Celkový přehled omezení Služeb
[bude doplněno]
7) Problémy a rizika
[bude doplněno]
8) Zpráva o stavu bezpečnosti
[bude doplněno]
9) Smluvní pokuty

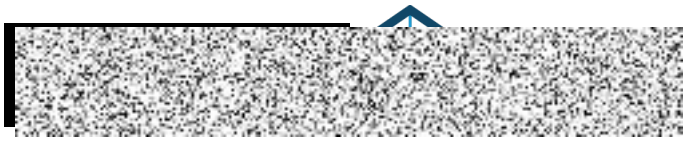


[bude doplněno]		
Seznam příloh		
P. č.	**Název přílohy**	
1	[bude doplněno]	
Schvalovací doložka		
Jméno a příjmení	**Organizace**	**Datum a podpis**
[bude doplněno]	Objednatel	[elektronický podpis včetně data podpisu]
[bude doplněno]	Poskytovatel	[elektronický podpis včetně data podpisu]

Příloha č. 13: Jednotkové ceny pro Služby

	Popis rozsahu Služby	Kč bez DPH	v Kč včetně DPH
Služba KL01	**Rozsah jednotek bezpečnostního monitoringu pro stanovení jednotkové ceny**	**v Kč bez DPH za 1 jednotku za měsíc**	**v Kč včetně DPH za 1 jednotku za měsíc**
Bezpečnostní monitoring (jednotka – počet událostí za vteřinu)	1–500	1 064,73 Kč	1 288,32 Kč
	501 - 1 000	483,80 Kč	585,40 Kč
	1 001 - 2 000	334,20 Kč	404,38 Kč
	2 001 - 5 000	242,48 Kč	293,40 Kč
	5 001 - 10 000	204,04 Kč	246,89 Kč
	10 001 - 15 000	190,33 Kč	230,30 Kč
	15 001 - 20 000	185,24 Kč	224,14 Kč
	20 001 - 25 000	181,80 Kč	219,98 Kč
	25 001 - 30 000	180,11 Kč	217,93 Kč
	30 001 - 40 000	177,70 Kč	215,02 Kč
Doplňkové služby KL01	**Rozsah Služby**	**v Kč bez DPH za měsíc**	**v Kč včetně DPH za měsíc**
Bezpečnostní monitoring databází	1 ks/databáze	26 602,91 Kč	32 189,52 Kč
Virtuální kolektor – Bezpečnostní monitoring databází	1 ks/kolektor	10 719,93 Kč	12 971,12 Kč
Virtuální agregátor – Bezpečnostní monitoring databází	1 ks/agregátor	10 719,93 Kč	12 971,12 Kč
Virtualizace DB – Virtuální kolektor pro Bezpečnostní monitoring databází	virtualizace pro 1 kolektor (32 BB, 600 GB)	12 765,40 Kč	15 446,13 Kč
Virtualizace DB – Virtuální agregátor pro Bezpečnostní monitoring databází	virtualizace pro 1 agregátor (32 BB, 1 536 GB)	15 469,50 Kč	18 718,10 Kč
Virtuální kolektor – Bezpečnostní monitoring	1 ks/kolektor	1 965,55 Kč	2 378,32 Kč
Virtuální procesor – Bezpečnostní monitoring	1 ks/procesor	1 965,55 Kč	2 378,32 Kč
Virtualizace BM – Virtuální kolektor pro Bezpečnostní monitoring	virtualizace pro 1 kolektor (64 BB, 512 GB)	10 443,20 Kč	12 636,27 Kč
Virtualizace BM – Virtuální procesor pro Bezpečnostní monitoring	virtualizace pro 1 procesor (112 BB, 1 024 GB)	18 645,30 Kč	22 560,81 Kč
Úložný prostor	256 GB	739,60 Kč	894,92 Kč

	Popis rozsahu Služby	Kč bez DPH	v Kč včetně DPH
Služba KL02	**Rozsah Služby**	**v Kč bez DPH za 1 GB za měsíc**	**v Kč včetně DPH za 1 GB za měsíc**
Logmanagement	1 GB uložených dat	1,992 Kč	2,41 Kč
Služba KL03	**Rozsah jednotek pro stanovení jednotkové ceny**	**v Kč bez DPH za 1 jednotku za měsíc**	**v Kč včetně DPH za 1 jednotku za měsíc**
Řízení přístupu a Session Recording (jednotka – počet souběžných uživatelů)	1–50	3 984,32 Kč	4 821,03 Kč
	51–100	2 537,65 Kč	3 070,56 Kč
	101–150	2 248,32 Kč	2 720,47 Kč
	151–200	2 124,32 Kč	2 570,43 Kč
	201–250	2 055,43 Kč	2 487,07 Kč
	251–300	2 011,59 Kč	2 434,02 Kč
Doplňkové Služby KL03	**Rozsah Služby**	**v Kč bez DPH za měsíc za balíček dle rozsahu**	**v Kč včetně DPH za měsíc**
Password Management (jednotka – počet uživatelů)	balíček 25	12 197,96 Kč	14 759,53 Kč
	balíček 50	22 058,78 Kč	26 691,12 Kč
	balíček 75	30 219,86 Kč	36 566,03 Kč
	balíček 100	37 106,13 Kč	44 898,42 Kč
	balíček 125	43 011,78 Kč	52 044,25 Kč
	balíček 150	48 146,95 Kč	58 257,81 Kč
	balíček 175	52 665,73 Kč	63 725,53 Kč
	balíček 200	56 683,69 Kč	68 587,26 Kč
	balíček 225	60 289,22 Kč	72 949,96 Kč
	balíček 250	63 551,05 Kč	76 896,77 Kč
	balíček 275	66 523,44 Kč	80 493,36 Kč
	balíček 300	69 249,83 Kč	83 792,29 Kč
Služba KL04	**Rozsah Služby**	**v Kč bez DPH za měsíc**	**v Kč včetně DPH za měsíc**
Kompetenční centrum KB (jednotka – počet dokumentů)	SŘBI do správy 25 dokumentů	234 824,36 Kč	284 137,48 Kč
	SŘBI do správy 50 dokumentů	261 756,86 Kč	316 725,80 Kč
	SŘBI do správy 75 dokumentů	288 689,36 Kč	349 314,13 Kč
	SŘBI do správy 100 dokumentů	378 464,36 Kč	457 941,88 Kč
	SŘBI do správy 150 dokumentů	468 239,36 Kč	566 569,63 Kč
	SŘBI do správy 200 dokumentů	522 104,36 Kč	631 746,28 Kč
	Rozsah Služby	**v Kč bez DPH za akceptované člověkodny odborných rolí**	**v Kč včetně DPH za akceptované člověkodny odborných rolí**
	SŘBI – metodická podpora	cena dle rozsahu a akceptace – dle sazby za 1 člověkoden uvedené v Ceníku rolí	



	Popis rozsahu Služby	Kč bez DPH	v Kč včetně DPH
Služba KL05	**Rozsah Služby**	**v Kč bez DPH za 1 člověkoden**	**v Kč včetně DPH za 1 člověkoden**
Konzultace	Konzultace nad rámec Služeb dle KL01 – KL04, KL06 – KL07	cena dle rozsahu a akceptace – dle sazby za 1 člověkoden uvedené v Ceníku rolí	
	Ceník rolí – název role	**v Kč bez DPH za 1 člověkoden**	**v Kč včetně DPH za 1 člověkoden**
	Analytik kybernetické bezpečnosti	13 100,00 Kč	15 851,00 Kč
	Architekt KB	16 900,00 Kč	20 449,00 Kč
	Manažer kybernetické bezpečnosti	13 800,00 Kč	16 698,00 Kč
	Manažer řízení rizik KB	12 100,00 Kč	14 641,00 Kč
	Organizátor vzdělávacích aktivit KB	11 400,00 Kč	13 794,00 Kč
	Manažer rozvoje služeb KB	14 200,00 Kč	17 182,00 Kč
	Bezpečnostní administrátor ICT	12 600,00 Kč	15 246,00 Kč
	Správce zranitelností	11 900,00 Kč	14 399,00 Kč
	Správce identit	12 900,00 Kč	15 609,00 Kč
	Administrátor unix	13 400,00 Kč	16 214,00 Kč
	Administrátor aplikace	11 400,00 Kč	13 794,00 Kč
	IT Analytik / IT architekt	14 200,00 Kč	17 182,00 Kč
Služba KL06	**Rozsah Služby**	**v Kč bez DPH za měsíc**	**v Kč včetně DPH za měsíc**
Vulnerability management	1 CI	332,02 Kč	401,74 Kč
Vulnerability management – engine	1 ks engine	11 789,02 Kč	14 264,71 Kč
Virtualizace pro nasazení 1 engine	virtualizace pro 1 ks engine (4 BB, 100 GB, správa)	4 678,10 Kč	5 660,50 Kč
Úložný prostor	256 GB	739,60 Kč	894,92 Kč
Služba KL07	**Rozsah Služby**	**v Kč bez DPH za měsíc**	**v Kč včetně DPH za měsíc**
Správa syslog serverů	Správa syslog serverů	73 590,00 Kč	89 043,90 Kč

Princip stanovení cen je popsán v Příloze č. 1–7 této Smlouvy.