SMLOUVA
o poskytování služby SOC

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“),
mezi:

Českou národní bankou
Na Příkopě 28
115 03 Praha 1
zastoupenou: Ing. Milanem Zirnsákem, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní
IČO: 48136450
DIČ: CZ48136450

(dále jen „objednatel“ nebo „ČNB“)

a

T-Mobile Czech Republic a.s.
zapsanou v obchodním rejstříku vedeném Městským soudem v Praze oddíl B vložka 3787
sídlo/místo podnikání: Tomíčkova 2144/1, 148 00 Praha 4
IČO: 64949681
DIČ: CZ64949681
zastoupenou: Ing. Jiřím Bunešem, na základě pověření
č. účtu: 19-2271190247/0100

(dále jen „poskytovatel“).

Preambule

Objednatel provozuje systém managementu bezpečnostních informací a událostí SIEM (dále jen „SIEM“) založený na produktu ArcSight a systém pro monitoring síťového provozu a detekci anomálií (dále jen „FlowMon“).

Vzhledem k celosvětově stoupajícímu trendu kybernetických útoků je potřeba zajistit nepřetržitý monitoring a kvalitní analýzu bezpečnostních událostí s využitím systému SIEM objednatele včetně návrhu na protiopatření 24 hodin denně 7 dnů v týdnu po celý rok. Rovněž je potřeba zajistit průběžnou úpravu pravidel v systému SIEM, aby byl schopen odhalovat nové hrozby, případně se zrychlilo jejich odhalení.

Článek I
Předmět smlouvy

1. Poskytovatel se touto smlouvou zavazuje poskytovat objednateli za sjednaných podmínek, na vlastní náklady a na své nebezpečí službu zahrnující:
   a) nepřetržitý vzdálený dohled/monitoring bezpečnostních událostí s využitím systému SIEM objednatele, a to 24 hodin denně 7 dnů v týdnu po celý rok,
   b) proaktivní vyhledávání a analýzu potenciálních bezpečnostních událostí KBU v pracovních dnech, na základě znalosti o nových typech útoků, znalosti systémového

prostředí ČNB, případně jiných podezřelých bezpečnostních událostí, které SIEM nedetekuje nebo negeneruje alert,

c) proaktivní vyhledávání konfiguračních chyb z bezpečnostních logů monitorovaných systémů v režimu minimálně 1h týdně,
d) detailní analýzu KBU dle operativně zaslaného požadavku osobami k tomu oprávněnými dle komunikační matice (viz příloha č. 6),
e) analýzu KBU zachycených systémem SIEM objednatele, včetně návrhu na protiopatření (řešení),
f) upozornění objednatele na zjištěné bezpečnostní incidenty (KBU/KBI) dle jejich závažnosti a v této smlouvě dohodnuté komunikační matice (viz příloha č. 6),
g) vylepšování bezpečnostního monitoringu v systému SIEM objednatele (pravidla, reporty, alerty apod.),
h) analytickou pomoc v případě potvrzeného kybernetického útoku,
i) poskytování pravidelného měsíčního reportu v souladu s požadavky objednatele dle specifikace v příloze č. 2, popř. dle bližšího popisu v příloze č. 6,
j) poskytování konzultačních služeb při případné úpravě pravidel, reportů a filtrů pro systém SIEM objednatele, které nespadají do plnění uvedeného v písm. a) až i) výše, v rozsahu 96 člověkohodin ročně,
k) poskytování konzultačních služeb při případné úpravě pravidel, reportů a filtrů pro systém SIEM objednatele, které jsou nad rámec rozsahu člověkohodin dle písm. j) tohoto odstavce. V případě potřeby budou tyto služby prováděny na základě nabídky poskytovatele, jejíž součástí bude předpokládaná pracnost a harmonogram realizace požadované služby. V případě akceptace nabídky objednatelem bude na tyto služby vystavena samostatná objednávka.

(dále též „služba“).

2. Podrobná specifikace a parametry poskytované služby dle odst. 1 jsou uvedeny v přílohách č. 1 a 6, a to v souladu s požadavky uvedenými v příloze č. 2.

3. Předmětem této smlouvy je dále závazek poskytovatele provést před zahájením poskytování služby dle odst. 1 přípravné činnosti specifikované v čl. II.

4. Součásti služby uvedené v odst. 1 písm. a) až i) tohoto článku budou poskytována výhradně formou vzdáleného přístupu. Definice a parametry vzdáleného přístupu jsou uvedeny v příloze č. 5 části A (příloha č. 5 část A a příloha č. 5 část B dále společně jako „příloha č. 5“). Náklady na zajištění vzdáleného přístupu až k přístupovému bodu vzdáleného přístupu (dále jen „VPN“) na perimetru ČNB hradí poskytovatel.

5. Poskytovatel bere na vědomí, že mu nebudou v rámci plnění zasílána žádná data, s výjimkou alertů generovaných systémem SIEM objednatele. Do kompletního prostředí systému SIEM a FlowMon bude poskytovateli umožněno přistupovat pouze prostřednictvím VPN bez možnosti uchovávat data u poskytovatele. Bližší popis zasílání dat viz příloha č. 6.

6. Za výše uvedená plnění se objednatel zavazuje uhradit ceny dle čl. V.

Článek II
Přípravné činnosti

1. Před zahájením poskytování služby dle čl. I odst. 1 písm. a) až k) budou realizovány níže uvedené přípravné činnosti rozdělené do tří etap, které budou předmětem akceptace dle čl. IV.

2. Etapa 1 – Realizační studie

2.1 První etapa je zaměřena na detailní analýzu požadavků objednatele na službu (příloha č. 2) a navrženého řešení služby poskytovatelem (příloha č. 1) s cílem ověřit realizovatelnost nabízené služby v podmínkách objednatele, ověřit a dokladovat soulad s požadavky objednatele, podrobně specifikovat technickou realizaci služby a případně identifikovat technické problémy či dosud neidentifikované změny a požadavky, které by vznikly v souvislosti s implementací a provozováním služby v prostředí objednatele.

2.2 Výstupem této etapy bude podrobná realizační studie, pro jejíž tvorbu využije poskytovatel šablonu realizační studie, uvedenou v příloze č. 8.

2.3 Sběr informací, které bude poskytovatel potřebovat pro vytvoření objednatelem požadované realizační studie, bude probíhat formou interview mezi odbornými pracovníky obou smluvních stran v místě plnění.

2.4 Z realizační studie musí být objednatel schopen ověřit, že navrhovaná služba a způsob jejího poskytování splňuje požadavky objednatele, vyhovuje jeho potřebám, jeho provozním zvyklostem a je implementovatelná ve lhůtách uvedených v této smlouvě. Dále u případně nově identifikovaných požadavků či změn souvisejících s implementací a provozováním služby v prostředí objednatele neuvedených v příloze č. 2 musí realizační studie obsahovat návrh vypořádání takových požadavků či změn. Řešení požadavků objednatele musí být v realizační studii popsáno tak, aby bylo zřejmé, že respektuje systémové prostředí objednatele a všechny jeho komponenty popsané v příloze č. 5, resp. že bude v systémovém prostředí objednatele funkční a nebude systémové prostředí objednatele ani jeho komponenty ohrožovat nebo poškozovat.

2.5 Tato etapa v sobě zahrnuje zejména následující činnosti:

a) seznámení odborných pracovníků poskytovatele s výpočetním prostředím ČNB, kritičností jednotlivých dozorovaných IT, IS a aplikací,
b) seznámení se s konfigurací systému SIEM objednatele (reporty, alerty, pravidla, korelace atd.),
c) návrh nových, případně úpravy stávajících pravidel v SIEM objednatele pro detekci KBU/KBI včetně priority implementace, aby byla zajištěna kvalita poskytované služby,
d) návrh na připojení nových zdrojů událostí, je-li to potřeba pro zajištění kvality poskytované služby,
e) definování způsobů vzájemné komunikace obou smluvních stran (komunikační matice) a eskalace,
f) definování struktury a obsahu měsíčního reportu,
g) vytvoření realizační studie,
h) ve spolupráci obou smluvních stran akceptaci realizační studie,
i) uzavření ujednání o zpracování osobních údajů v souladu s přílohou č. 4.

2.6 Akceptovaná realizační studie je pro poskytovatele závazná a stává se volně připojenou přílohou č. 6 této smlouvy.

2.7 Činnosti prováděné v rámci této etapy se realizují v pracovní dny během standardní pracovní doby objednatele (7:45 až 16:15 hodin – časové pásmo místa plnění), pokud se obě smluvní strany nedohodnou jinak.

3. **Etapa 2 – Implementace**

   3.1 Tato etapa je zaměřena na technické zprovoznění služby spočívající v potřebné konfiguraci zabezpečeného VPN a prioritní úpravy obsahu SIEM v prostředí objednatele a instalaci a konfiguraci VPN v prostředí poskytovatele, dále pak nastavení a aktivaci monitorovacích a reportovacích procesů, a to vše v souladu s přílohou č. 6.

   3.2 Druhá etapa zahrnuje následující činnosti objednatele, k nimž poskytovatel poskytne objednateli potřebnou součinnost:

   a) zajištění přístupů jednotlivých pracovníků poskytovatele, kteří se budou podílet na poskytování částí služby dle čl. I odst. 1 písm. a) až i):
      - aktivace přístupů do konzole SIEM objednatele formou VPN,
      - aktivace přístupů do konzole FlowMon objednatele formou VPN,
      - aktivace přístupů do sdíleného úložiště Citrix ShareFile,
      - předání certifikátů pracovníkům poskytovatele na jejich vlastní čipovou kartu (token) dle specifikace uvedené v příloze č. 2 (požadavek S33) pro zajištění bezpečného přihlášení ke konzoli SIEM a FlowMon objednatele prostřednictvím VPN;

   b) úprava stávajících pravidel v SIEM objednatelem, dle doporučení a podrobného návodu poskytovatele uvedeného v realizační studii;

   a dále následující činnosti poskytovatele:

   c) zprovoznění VPN u poskytovatele dle návodu od objednatele v souladu s technickou specifikací uvedenou v příloze č. 2 (požadavek S31),

   d) vytvoření nových pravidel v SIEM objednatele navržených v realizační studii s nejvyšší prioritou nebo dodání těchto pravidel formou instalačních balíčků pro nástroj ArcSight.

4. **Etapa 3 - Ověřovací provoz**

   Po dobu 3 měsíců od podpisu dílčího akceptačního protokolu druhé etapy bude bez přerušení probíhat ověřovací provoz v režimu poskytování částí služby dle čl. I odst. 1 písm. a) až i) a za součinnosti poskytovatele, spočívající v odstraňování vad implementace, včetně obsahu měsíčního reportu.

Článek III
Lhůty, místo plnění a pověřené osoby

1. Poskytovatel se zavazuje zahájit poskytování služby v jejím celku dle čl. I odst. 1 písm. a) až k) do 8 měsíců ode dne podpisu této smlouvy s tím, že první etapa dle čl. II bude dokončena (akceptována) nejpozději do 2 měsíců od podpisu smlouvy a druhá etapa dle čl. II bude dokončena (akceptována) nejpozději do 3 měsíců od akceptace první etapy.
2. Za místo plnění se považuje sídlo objednatele na adrese Na Příkopě 28, Praha 1.
3. Pověřenými osobami smluvních stran jsou:
   a) za objednatele:
   [redacted]
   b) za poskytovatele:
   [redacted]
4. Pověřené osoby podle předchozího odstavce tohoto článku zastávají funkci pověřených

osob podle této smlouvy pouze do okamžiku akceptace první etapy podle čl. IV. Akceptací první etapy se pověřenými osobami smluvních stran stávají pověřené osoby smluvních stran uvedené v komunikační matici realizační studie (příloha č. 6). Komunikační matice (viz příloha č. 6) může obsahovat bližší určení rozsahu pověření jednotlivých pověřených osob nebo jejich skupin formou odkazů na konkrétní ustanovení této smlouvy (vč. příloh).

5. V případě změny pověřených osob smluvních stran nebo jejich kontaktních údajů, popř. dalších osob či kontaktních údajů uvedených v komunikační matici, jsou smluvní strany povinny nahlásit změnu následující pracovní den po provedení změny na e-mailové adresy pověřených osob druhé smluvní strany. Změna je účinná dnem jejího oznámení druhé smluvní straně, a to bez povinnosti uzavírat dodatek k této smlouvě. Upravená komunikační matice vždy nahrazuje příslušnou část přílohy č. 6 této smlouvy.

Článek IV
Akceptace přípravných činností

1. Před ukončením každé etapy uvedené v článku II se uskuteční akceptační řízení. Akceptační řízení začne předložením všech potřebných podkladů k příslušnému předmětu akceptace kterékoliv pověřené osobě objednatele.
2. Při akceptačních řízeních budou vady odstraňovány a připomínky vypořádány bez zbytečného odkladu.
3. O ukončení každého akceptačního řízení bude sepsán akceptační protokol, který vyhotoví objednatel. K akceptačnímu protokolu se vyjádří poskytovatel nejpozději do 3 pracovních dnů po jeho obdržení. Pokud tak neučiní, má se za to, že s uvedeným závěrem souhlasí. Akceptační protokoly podepisují pověřené osoby smluvních stran (postačuje jedna z nich za každou smluvní stranu).
4. Kterákoliv etapa bude považována za úspěšně provedenou, pokud bude prostá vad, druhou etapu lze akceptovat s výhradami. Akceptační protokol v případě akceptace s výhradami musí obsahovat výčet vad, způsob a lhůtu pro jejich odstranění. Pokud objednatel pro vady kteroukoliv etapu neakceptuje, uvede to v akceptačním protokolu spolu s odůvodněním.
5. Poskytovatel je oprávněn zahájit další etapu až poté, co objednatel akceptoval předchozí etapu. Zahájení poskytování služby podle čl. I odst. 1 je podmíněno akceptací třetí etapy.

Akceptace první etapy

6. Po realizaci všech činností v rámci první etapy předloží poskytovatel objednateli realizační studii k připomínkám v elektronické podobě, ve formátech MS Office nebo PDF.
7. Objednatel uplatní písemně (poštou nebo elektronicky) připomínky nejpozději do 7 pracovních dnů od obdržení realizační studie.
8. Za vadu realizační studie se považuje zejména:
    a) chybějící textová část dokumentace nebo nevyplněná či nevypracovaná část realizační studie, jejíž předepsaná struktura je uvedena v příloze č. 8,
    b) textová část realizační studie neodpovídá skutečnosti popisované entity (např. systému, procesu, chybové zprávě, skutečnostem nebo požadavkům uvedeným v přílohách č. 1 a 2) nebo je v rozporu s některým z povinných požadavků dle přílohy č. 2.
9. Poskytovatel předloží objednateli vypořádání připomínek v elektronické podobě, ve formátech MS Office nebo PDF do 5 pracovních dnů od jejich obdržení.

10. Objednatel rozhodne o akceptaci či neakceptaci realizační studie do 7 pracovních dnů od okamžiku, kdy obdrží vypořádání připomínek. Během této doby si objednatel vyhrazuje právo pokládat další dotazy a návrhy na doplnění a úpravy studie (např. formou e-mailu) poskytovateli, které budou zodpovězeny či vypořádány poskytovatelem bez zbytečného odkladu.
11. Podmínkou akceptace první etapy je:
    a) realizační studie bez vad (akceptovaná),
    b) uzavřené ujednání o zpracování osobních údajů (příloha č. 4).
12. Objednatel je oprávněn kdykoliv před akceptací první etapy využít výhradu uvedenou v čl. XI odst. 6, a to zejména v případech, kdy je z realizační studie zřejmé, že kvalita nabízené služby neodpovídá zvyklostem a standardům objednatele, či v případě detekce dodatečných změn a nákladů uvedených v realizační studii, které by měly velké dopady na očekávaný rozpočet objednatele či zatížení jeho lidských zdrojů.
13. Dílčí akceptační protokol první etapy podepíše alespoň jedna pověřená osoba za každou smluvní stranu.

Akceptace druhé etapy

14. Po ukončení implementace a zprovoznění služby předloží poskytovatel objednateli výsledek jím provedených prací, zejména popis požadovaných úprav pravidel SIEM objednatele.
15. Akceptační řízení bude objednatelem provedeno do 5 pracovních dnů poté, co poskytovatel naplní podmínky dle předchozího odstavce tohoto článku.
16. Podmínkou akceptace druhé etapy je:
    a) ověření funkčního připojení k systému SIEM a FlowMon objednatele přes VPN z prostředí poskytovatele,
    b) ověření zasílání alertů ze SIEM objednatele do prostředí poskytovatele,
    c) ověření přístupu poskytovatele do sdíleného prostoru objednatele pro předávání dokumentů,
    d) dokončení instalace prioritních pravidel a úprav kontentu v SIEM objednatele (pravidla, reporty, alerty apod.).
17. Dílčí akceptační protokol druhé etapy podepíše alespoň jedna pověřená osoba za každou smluvní stranu. Následující den po podpisu dílčího akceptačního protokolu druhé etapy je zahájen ověřovací provoz.

Akceptace třetí etapy

18. V průběhu ověřovacího provozu předkládá poskytovatel objednateli měsíční reporty k připomínkám, které objednatel uplatní písemně (poštou nebo elektronicky) nejpozději do 5 pracovních dnů po obdržení reportu.
19. Rozhodnutí o akceptaci či neakceptaci reportu provede objednatel vždy do 5 pracovních dnů od obdržení vypořádání připomínek k příslušnému měsíčnímu reportu.
20. Za vadu měsíčního reportu z ověřovacího provozu se považuje zejména:
    a) absence některých částí podle struktury uvedené v realizační studii (příloha č. 6),
    b) opomenutí detekovaného KBU/KBI,

c) neúplné, chybné nebo nekonzistentní údaje.

21. Za vadu v ověřovacím provozu se považuje zejména:

    a) nedostupnost SIEM objednatele pro poskytovatele z důvodů na straně poskytovatele, v rozsahu větším než 2 hodiny,

    b) nedetekované KBU/KBI poskytovatelem, ačkoliv je objednatel detekoval.

22. Podmínkou akceptace třetí etapy je:

    a) všechny měsíční reporty bez vad (akceptované),

    b) úspěšně provedený ověřovací provoz, ve kterém nebyly detekovány vady, nebo byly všechny vady odstraněny do jeho ukončení.

23. Akceptací třetí etapy bude zahájeno poskytování služby v jejím celku dle čl. I odst. 1 písm. a) až k). Za den akceptace třetí etapy se považuje den, ke kterému byly naplněny podmínky akceptace třetí etapy. O akceptaci se sepíše akceptační protokol, který podepíše alespoň jedna pověřená osoba za každou smluvní stranu a ve kterém bude uveden nejméně den akceptace třetí etapy podle předchozí věty.

24. Pokud nebude ověřovací provoz ukončen akceptací třetí etapy, prodlužuje se ověřovací provoz o dobu dalších 3 měsíců a akceptace třetí etapy se opakuje. Ověřovací provoz lze prodloužit i opakovaně, nejsou-li však naplněny podmínky akceptace třetí etapy ani po 6 měsících ověřovacího provozu, je objednatel oprávněn od smlouvy odstoupit podle čl. XI odst. 4 písm. a). Prodloužením ověřovacího provozu nejsou dotčeny žádné další doby nebo lhůty podle této smlouvy.

Článek V
Cena a platební podmínky

1. Cena za přípravné činnosti dle čl. II činí celkem 0 Kč bez DPH, z toho činí cena za realizaci první etapy 0 Kč bez DPH a cena za realizaci druhé etapy 0 Kč bez DPH.

2. Cena za poskytování části služby v rámci ověřovacího provozu podle čl. I odst. 1 písm. a) až i) činí 24 625 Kč bez DPH měsíčně.

3. Cena za poskytování části služby po ukončení ověřovacího provozu podle čl. I odst. 1 písm. a) až j) činí 62 825 Kč bez DPH měsíčně.

4. Cena za poskytování části služby dle čl. I odst. 1 písm. k) bude stanovena jako součin počtu skutečně poskytnutých hodin konzultací a hodinové sazby, která činí 1 720 Kč bez DPH.

5. Cena dle odst. 1 za přípravné činnosti bude uhrazena na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve v den podpisu akceptačního protokolu třetí etapy.

6. Cena dle odst. 2 za poskytování části služby v rámci ověřovacího provozu bude hrazena na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve poslední den kalendářního měsíce, za který se platí. Výše paušální ceny za období kratší než kalendářní měsíc se vypočte jako alikvotní část měsíčního paušálu.

7. Cena dle odst. 3 za poskytování části služby po ukončení ověřovacího provozu bude hrazena na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve poslední den kalendářního měsíce, za který se platí. Výše paušální ceny za období kratší než kalendářní měsíc se vypočte jako alikvotní část měsíčního paušálu.

8. Úhrada ceny dle odst. 4 bude prováděna na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve poslední den kalendářního měsíce, ve kterém byly

konzultační služby poskytnuty. Přílohou daňového dokladu bude časový a věcný rozpis konzultací podepsaný pověřenou osobou objednatele.

9. K cenám bude připočtena DPH v sazbě platné ke dni uskutečnění zdanitelného plnění. Ceny zahrnují veškeré náklady poskytovatele spojené s plněním podle této smlouvy včetně nákladů na činnost, kterou poskytovatel vykonává jakožto zpracovatel osobních údajů podle ujednání (viz příloha č. 4).

10. Doklad k úhradě (fakturu) zašle poskytovatel elektronicky jako přílohu e-mailové zprávy na adresu faktury@cnb.cz ve formátu ISDOC. Pokud není možné vytvořit doklad ve formátu ISDOC, je možné zasílat jej ve formátu PDF. V jedné e-mailové zprávě smí být pouze jeden doklad k úhradě. Mimo vlastní doklad k úhradě může být přílohou e-mailové zprávy jedna až sedm příloh k dokladu ve formátech PDF, DOC, DOCX, XLS, XLSX. Přijaty budou i doklady k úhradě v jiném formátu, který bude v souladu s evropským standardem elektronické faktury. Nebude-li možné zaslat doklad k úhradě elektronicky, zašle jej poskytovatel v analogové formě na adresu:

    Česká národní banka
    sekce rozpočtu a účetnictví
    odbor účetnictví
    Na Příkopě 28
    115 Praha 1

11. Doklad k úhradě bude obsahovat údaje podle § 435 občanského zákoníku a bankovní účet, na který má být placeno a který je uveden v záhlaví této smlouvy nebo který byl později aktualizován poskytovatelem (dále jen „určený účet“). Daňový doklad bude nadto obsahovat náležitosti stanovené v zákoně o dani z přidané hodnoty. Nezbytnou náležitostí každého dokladu je také číslo této smlouvy (ve formátu ISDOC v poli ID ve skupině Contract References), nebo číslo objednávky (ve formátu ISDOC v poli External_Order_ID ve skupině OrderReference), jsou-li objednávky v rámci smlouvy vystavovány. Pokud doklad bude postrádat některou ze stanovených náležitostí nebo bude obsahovat chybné údaje, je objednatel oprávněn jej vrátit poskytovateli, a to až do lhůty splatnosti. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného dokladu.

12. V případě, že bude v dokladu k úhradě uveden jiný než určený účet, je pověřená osoba poskytovatele povinen na základě výzvy objednatele sdělit na e-mailovou adresu, ze které byla výzva odeslána, zda má být zaplaceno na bankovní účet uvedený v dokladu, nebo na určený účet. V tomto případě se doklad k úhradě nevrací s tím, že lhůta splatnosti začíná běžet až dnem doručení sdělení poskytovatele podle předchozí věty.

13. Splatnost dokladu k úhradě je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.

14. Smluvní strany se ve smyslu ustanovení § 1991 občanského zákoníku dohodly, že je objednatel oprávněn započíst jakoukoli svou peněžitou pohledávku za poskytovatelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce poskytovatele za objednatelem, ať splatné či nesplatné.

15. Poskytovatel je oprávněn navrhnout objednateli změnu cen podle odst. 3 a 4 tohoto článku v návaznosti na vývoj Indexu cen v tržních službách, stejné období předchozího roku = 100, konkrétně index J62 Služby v oblasti programování a poradenství a související služby, sloupec Průměr od počátku roku, a to průměr za předchozí kalendářní rok, který vyhlašuje Český statistický úřad. Úpravu cen je poskytovatel oprávněn navrhnout nejdříve v roce 2026. Úpravy cen budou prováděny písemnými dodatky ke smlouvě podepsanými oprávněnými zástupci obou smluvních stran.

Článek VI
Mlčenlivost, bezpečnostní požadavky objednatele a sociální odpovědnost poskytovatele

1. Poskytovatel se zavazuje zajistit, že on i veškeré osoby podílející se na jeho plnění dle této smlouvy zachovají mlčenlivost o všech skutečnostech, se kterými se seznámí v průběhu plnění této smlouvy a které nejsou veřejně dostupné. Povinnost mlčenlivosti trvá i po skončení platnosti smlouvy.
2. Poskytovatel a pracovníci či poddodavatelé poskytovatele a jejich pracovníci smí používat informace získané v souvislosti s plněním dle této smlouvy výhradně pro účely plnění této smlouvy. Dostane-li se kterákoliv z osob uvedených v tomto odstavci v průběhu plnění do kontaktu s údaji objednatele vyplývajícími z jeho provozní činnosti, zavazuje se tyto údaje nezneužít, nezměnit ani nijak nepoškodit, neztratit či znehodnotit.
3. Poskytovatel se zavazuje zajistit, aby jeho pracovníci či poddodavatelé poskytovatele a jejich pracovníci v plném rozsahu dodržovali bezpečnostní požadavky podle části 4. příloha č. 2, bezpečnostní požadavky objednatele podle přílohy č. 3 a obecná pravidla pro poskytovatele v oblasti bezpečnosti IT podle přílohy č. 7.
4. Objednatel je oprávněn kontrolovat plnění povinností podle odst. 3 tohoto článku stanovených pro zachování bezpečnosti objednatele, a to v místě sídla poskytovatele nebo i v jiném místě, kde dochází k činnostem poskytovatele či jeho poddodavatele spojených s plněním povinností poskytovatele podle této smlouvy. Poskytovatel za tímto účelem zajistí zástupcům objednatele, kteří budou provedením kontroly pověřeni, přístup ke všem relevantním informacím a na všechna příslušná místa tak, aby mohlo být řádně provedeno hodnocení naplnění povinností podle odst. 3 tohoto článku, resp. povinností vyplývajících z části 4. přílohy č. 2, přílohy č. 3 nebo přílohy č. 7. Poskytovatel poskytne objednateli na jeho žádost, resp. žádost pověřené osoby objednatele, veškeré podklady o přijatých a provedených technických a organizačních opatřeních k zajištění plnění předmětných povinností.
5. Poskytovatel se zavazuje, že v souvislosti s plněním dle této smlouvy zajistí legální zaměstnávání osob a férové a důstojné pracovní podmínky pro všechny pracovníky podílející se na plnění této smlouvy. Férovými a důstojnými pracovními podmínkami se přitom rozumí takové pracovní podmínky, které splňují alespoň minimální standardy stanovené pracovněprávními a mzdovými předpisy. Poskytovatel je povinen zajistit splnění požadavků dle tohoto ustanovení i u svých poddodavatelů.
6. Poskytovatel se zavazuje, že v souvislosti s plněním dle této smlouvy zajistí řádné a včasné plnění finančních závazků vůči svým poddodavatelům, kdy za řádné a včasné plnění se považuje plné uhrazení poddodavatelem vystavených faktur za plnění poskytnutá poskytovateli v souvislosti s touto smlouvou, a to nejpozději do 10 dnů od obdržení platby ze strany objednatele.
7. Objednatel je oprávněn plnění povinností dle odst. 5 nebo 6 tohoto článku smlouvy kdykoliv kontrolovat. Je-li k provedení této kontroly potřeba předložení dokumentů, zavazuje se poskytovatel k jejich předložení nejpozději do 5 pracovních dnů od doručení výzvy objednatele.

Článek VII
Odstraňování vad služby

1. V případě, že poskytování služby nebude odpovídat podrobné specifikaci a parametrům poskytované služby, které jsou uvedeny v přílohách č. 1 a 6, nebo nebude v souladu

s požadavky uvedenými v příloze č. 2, půjde o vadu. Odstraněním vady se rozumí též poskytnutí řešení, které vykazuje z pohledu uživatele shodnou nebo obdobnou funkčnost.

2. Zjištěnou vadu oznamuje objednatel poskytovateli buď telefonicky s následným potvrzením elektronickou poštou, nebo oznámení o vadě provede prostřednictvím Help-deskového systému poskytovatele, a to v souladu s komunikační maticí (viz příloha č. 6).
3. Poskytovatel potvrdí příjem oznámení o vadě nejpozději do 4 hodin od jejího zaslání objednatelem. Vady mohou být odstraňovány jen v pracovní dny v době od 8:00 do 16:15 hodin a pracovníci poskytovatele jsou povinni vadu odstranit bez zbytečného odkladu a bez neodůvodněného přerušení v poskytování služby, nejpozději však do 5 pracovních dnů od potvrzení o přijetí oznámení o vadě, nedohodnou-li se pověřené osoby smluvních stran jinak.
4. Komunikace v průběhu řešení vady probíhá v souladu s komunikační maticí (viz příloha č. 6).

Článek VIII
Kybernetická bezpečnost

1. Poskytovatel je při plnění této smlouvy v postavení významného dodavatele ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 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), ve znění pozdějších předpisů (dále jen „VKB“), a bere na vědomí, že po dobu účinnosti této smlouvy bude veden v evidenci významných dodavatelů objednatele ve smyslu § 8 odst. 1 písm. b) a c) VKB.
2. Rozsah zapojení poskytovatele na zajištění bezpečnosti aktiv informačních systémů kritické informační infrastruktury a aktiv významných informačních systémů používaných v prostředí objednatele je určen předmětem této smlouvy.
3. Poskytovatel se zavazuje při výkonu své činnosti včas a prokazatelně upozornit objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k pravidlům bezpečnosti, jejichž následkem může vzniknout újma nebo nesoulad s právními předpisy, a zajistit ve spolupráci s objednatelem náhradní způsob naplnění pravidel bezpečnosti, pokud stávající řešení přestalo být funkční a efektivní.
4. Poskytovatel se zavazuje informovat objednatele o tom, jakým způsobem řídí bezpečnostní rizika spojená s plněním předmětu této smlouvy a dále jaká jsou zbytková rizika související s plněním této smlouvy.
5. Dojde-li u poskytovatele k výskytu bezpečnostních incidentů vzniklých v souvislosti s plněním této smlouvy, zavazuje se poskytovatel o těchto bezpečnostních incidentech bezodkladně informovat objednatele. Poskytovatel se dále zavazuje oznamovat objednateli bezodkladně neobvyklé chování informačních systémů, jichž se plnění dle této smlouvy týká, a podezření na jakékoliv zranitelnosti bezpečnosti informací.
6. Poskytovatel se zavazuje informovat objednatele o významné změně ovládání poskytovatele. Ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů či ekvivalentní postavení, a to do 5 pracovních dnů od uskutečnění této změny.
7. Poskytovatel se zavazuje informovat objednatele o změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými poskytovatelem k plnění této smlouvy, a to do 5 pracovních dnů od uskutečnění této změny.

Článek IX
Mezinárodní sankce

1. Poskytovatel potvrzuje, že ke dni podpisu této smlouvy on ani jeho poddodavatelé nenaplňují definiční znaky subjektů uvedených v čl. 5k nařízení (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění jeho změn (dále také jako „nařízení č. 833/2014“), nebo subjektů uvedených v čl. 1h rozhodnutí Rady 2014/512/SZBP ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění jeho změn (dále jen „rozhodnutí 2014/512/SZBP“), kterým je zakázáno zadat či plnit jakoukoli veřejnou zakázku nebo koncesní smlouvu ve smyslu v tomto ustanovení uvedeného nařízení či rozhodnutí. Subjekty naplňující definiční znaky subjektů uvedených v čl. 5k nařízení č. 833/2014 nebo subjektů uvedených v čl. 1h rozhodnutí 2014/512/SZBP budou dále označovány jako „určené subjekty“.

2. Poskytovatel dále potvrzuje, že ke dni podpisu této smlouvy není osobou uvedenou v příloze I nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění jeho změn (dále také jako „nařízení č. 269/2014“), nebo v příloze I nařízení Rady (EU) č. 208/2014 ze dne 6. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, ve znění jeho změn (dále také jako „nařízení č. 208/2014“), nebo v příloze I nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska, ve znění jeho změn (dále také jako „nařízení č. 765/2006“), nebo v příloze rozhodnutí Rady 2014/145/SZBP ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění jeho změn (dále také jako „rozhodnutí 2014/145/SZBP“). Osoba uvedená v příloze I nařízení č. 269/2014 nebo v příloze I nařízení č. 208/2014 nebo v příloze I nařízení č. 765/2006 nebo v příloze rozhodnutí Rady 2014/145/SZBP bude dále označována jako „určená osoba“.

3. Poskytovatel se současně zavazuje, že určeným osobám dle předchozího odstavce (není-li jí sám) nebo v jejich prospěch nezpřístupní žádné finanční prostředky ani hospodářské zdroje získané v souvislosti s plněním dle této smlouvy, a to přímo ani nepřímo.

4. Poskytovatel dále potvrzuje, že plnění jím poskytované dle této smlouvy neporušuje žádným způsobem jakékoliv platné právní předpisy vydané zejména orgány Evropské unie [tj. zejména zákazy dovozu výrobků ze železa a oceli ve smyslu nařízení Rady (EU) č. 2022/428 ze dne 15. března 2022, kterým se mění „základní“ nařízení (EU) č. 833/2014, nebo nařízení Rady (EU) č. 2022/355 ze dne 2. března 2022, kterým se mění „základní“ nařízení (ES) č. 765/2006 o omezujících opatřeních vzhledem k situaci v Bělorusku apod.]. Objednatel je oprávněn při porušení této povinnosti poskytovatele plnění nepřevzít v jakékoliv jeho části.

5. V případě, že by v průběhu účinnosti této smlouvy poskytovatel nebo jeho jakýkoliv poddodavatel naplnili definiční znaky určeného subjektu nebo se poskytovatel stal určenou osobou, je poskytovatel povinen o takové skutečnosti objednatele bez zbytečného odkladu, nejpozději do 2 pracovních dnů od nastání takové skutečnosti, písemně informovat.

6. Dojde-li za dobu účinnosti této smlouvy ke změnám v kterémkoliv z výše uvedených nařízení Rady (EU) či rozhodnutí Rady nebo k přijetí jakékoliv jiné nové legislativy tak, že bude nezbytné dát tuto smlouvu s nařízením Rady (EU), rozhodnutím Rady nebo jinou novou legislativou do souladu, zavazují se smluvní strany uzavřít písemný dodatek k této

smlouvě, jehož předmětem bude úprava či doplnění práv a povinností smluvních stran v rámci této smlouvy (sankční mechanismy či nové možnosti ukončení smlouvy z toho nevyjímaje), a to bez zbytečného odkladu, nejpozději do 15 pracovních dnů poté, co změny nařízení Rady (EU), rozhodnutí Rady či jiná nová legislativa nabydou platnosti, nedohodnou-li se smluvní strany jinak.

7. Vznikne-li objednateli v souvislosti s nepravdivým prohlášením nebo porušením povinností poskytovatele dle tohoto článku smlouvy jakákoliv škoda, je poskytovatel tuto škodu objednateli povinen v plné výši nahradit.

Článek X
Smluvní pokuty, úrok z prodlení

1. V případě prodlení poskytovatele v kterékoliv lhůtě uvedené v čl. III odst. 1 je objednatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý den prodlení. To neplatí, pokud k prodlení poskytovatele došlo z důvodů na straně objednatele; prodloužení ověřovacího provozu v souladu s čl. IV odst. 24 není důvodem na straně objednatele.
2. V případě porušení povinností poskytovatele podle čl. VI odst. 1, 2 nebo 3 nebo čl. VIII je objednatel oprávněn požadovat smluvní pokutu ve výši 20 000 Kč za každý jednotlivý zjištěný případ porušení této povinnosti; za porušení povinnosti poskytovatele se považuje i případ porušení mlčenlivosti nebo nedovolené použití informace jakoukoliv osobou, která se podílela na plnění této smlouvy ze strany poskytovatele, neprokáže-li poskytovatel, že tomuto porušení bránil všemi způsoby, které po něm lze spravedlivě požadovat, včetně uložení a příp. vymožení smluvní pokuty ve výši nejméně 20 000 Kč.
3. V případě porušení povinností poskytovatele podle čl. VI odst. 4 je objednatel oprávněn požadovat smluvní pokutu ve výši 5 000 Kč za každý takový případ a každý den, kdy porušení povinnosti trvá.
4. V případě prodlení poskytovatele se splněním smluvní povinnosti ve stanovené lhůtě dle čl. VI odst. 7, čl. XIII odst. 1 nebo čl. XIII odst. 4 písm. a) nebo b) je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každý den prodlení.
5. V případě prodlení poskytovatele v kterékoliv lhůtě stanovené v čl. VII odst. 3 je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každou i započatou hodinu, jedná-li se o prodlení s potvrzením příjmu oznámení o vadě, resp. za každý i jen započatý pracovní den, jedná-li se o prodlení s odstraněním vady.
6. V případě prodlení poskytovatele v kterékoliv lhůtě dle čl. IX této smlouvy je objednatel oprávněn požadovat po poskytovateli smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
7. V případě, že se ukáže jakékoliv tvrzení poskytovatele uvedené v čl. IX této smlouvy jako nepravdivé nebo poruší-li poskytovatel závazek stanovený v čl. IX této smlouvy, vzniká objednateli nárok na smluvní pokutu ve výši 100 000 Kč za každé jednotlivé nepravdivé tvrzení poskytovatele či za každé jednotlivé porušení závazku poskytovatele.
8. V případě prodlení poskytovatele ve lhůtě uvedené v bodě 2. písm. g) přílohy č. 2 je objednatel oprávněn požadovat smluvní pokutu ve výši 2 000 Kč za každou i započatou hodinu prodlení, nejvýše však 48 000 Kč za měsíc.
9. V případě porušení povinnosti stanovené v bodě 3. písm. a) přílohy č. 2 je objednatel oprávněn požadovat smluvní pokutu ve výši 5 000 Kč za každé takové porušení.

10. V případě opakovaně vadného plnění (nekvalitní nebo neúplné) analýzy KBU/KBI, dle bodu 2. písm. j) a k) přílohy č. 2 je objednatel oprávněn požadovat smluvní pokutu ve výši 5 000 Kč za každý takový případ.
11. V případě porušení jakékoli povinnosti stanovené v bodě 4. přílohy č. 2, příloze č. 3 nebo příloze č. 7 je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každé takové porušení.
12. V případě prodlení objednatele s uhrazením daňového dokladu je poskytovatel oprávněn požadovat úrok z prodlení podle předpisů občanského práva.
13. Smluvní pokuta i úrok z prodlení jsou splatné do 14 dnů od doručení příslušného dokladu povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.
14. Smluvní pokutou není dotčen nárok na náhradu škody. Případná odpovědnost poskytovatele za škodu způsobenou neplněním povinností vyplývajících z této smlouvy je omezena celkovou částkou ve výši 20 000 000 Kč, kterou smluvní strany považují za předvídatelnou škodu.

Článek XI
Trvání a výpověď smlouvy, odstoupení od smlouvy, zrušení smlouvy zaplacením odstupného

1. Smlouva se uzavírá na dobu neurčitou.
2. Smlouvu lze ukončit písemnou výpovědí bez uvedení důvodu. Výpovědní doba činí v případě objednatele 3 měsíce, v případě poskytovatele 12 měsíců. Výpovědní doba počíná běžet prvním dnem kalendářního měsíce následujícího po doručení písemné výpovědi druhé smluvní straně. Poskytovatel může vypovědět smlouvu nejdříve po 3 letech od zahájení poskytování služby.
3. Smluvní strany se dohodly, že objednatel je oprávněn kdykoliv v průběhu insolvenčního řízení zahájeného na majetek poskytovatele vypovědět tuto smlouvu, a to v 14denní výpovědní době, která počíná běžet dnem následujícím po doručení písemné výpovědi poskytovateli
4. V případě, že některá ze smluvních stran poruší podstatným způsobem smluvní povinnost vyplývající pro ni z této smlouvy, je druhá smluvní strana oprávněna od smlouvy odstoupit nebo ji vypovědět bez výpovědní doby. Objednatel je oprávněn odstoupit i od části smlouvy. Za podstatné porušení smluvní povinnosti strany považují zejména tyto případy:
    a) ověřovací provoz probíhá po dobu delší než 6 měsíců a přesto nejsou naplněny podmínky akceptace třetí etapy,
    b) poskytovatel je v prodlení v kterékoliv lhůtě uvedené v článku III odst. 1 této smlouvy delším než 1 měsíc,
    c) poskytovatel poruší jakoukoliv svojí povinnost podle čl. VI odst. 1 až 4 nebo čl. VIII,
    d) poskytovatel odmítne uzavřít nebo jinak znemožní uzavření dodatku s objednatelem podle čl. XIII odst. 2,
    e) porušení jakékoliv povinnosti poskytovatele podle čl. XIII odst. 4 písm. a) až d) včetně prodlení ve lhůtě ke splnění takové povinnosti delším než 5 pracovních dnů,
    f) neuzavření, ukončení nebo porušení podmínek sjednaných ve smlouvě o zpracování osobních údajů,

g) objednatel je v prodlení s úhradou kterékoliv platby dle této smlouvy delším než 30 dnů.

5. Objednatel je dále oprávněn odstoupit od smlouvy, pokud dojde k významné změně kontroly nad poskytovatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů či ekvivalentní postavení nebo dojde ke změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými poskytovatelem k plnění této smlouvy a tato změna bude objednatelem vyhodnocena jako bezpečnostní riziko ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a/nebo VKB

6. V souladu s ustanovením § 1992 občanského zákoníku si smluvní strany sjednávají, že objednatel je oprávněn zrušit tuto smlouvu zaplacením odstupného ve výši 30 000 Kč na účet poskytovatele, a to kdykoliv před akceptací realizační studie (první etapa). Zrušení smlouvy je účinné zaplacením sjednaného odstupného na bankovní účet poskytovatele, č. ú.: 19-2271190247/0100. Zaplacením odstupného zanikají všechna práva a povinnosti obou smluvních stran vyplývající ze zrušené smlouvy s výjimkou závazku mlčenlivosti poskytovatele.

7. Odstoupení od smlouvy je účinné dnem doručení oznámení o odstoupení od smlouvy druhé smluvní straně. Výpověď bez výpovědní doby podle odst. 2 tohoto článku je účinná dnem doručení druhé smluvní straně.

8. Skončením smlouvy nejsou dotčena ustanovení týkající se vyrovnání smluvních závazků, smluvních pokut, závazku mlčenlivosti poskytovatele a ustanovení týkající se takových práv a povinností, z jejichž povahy vyplývá, že mají trvat i po skončení smlouvy.

Článek XII
Uveřejnění smlouvy a skutečně uhrazené ceny za plnění smlouvy

1. Poskytovatel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu včetně všech jejích případných změn a dodatků a výši skutečně uhrazené ceny za plnění této smlouvy.

2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele v době uzavření této smlouvy je https://ezak.cnb.cz/.

3. Povinnost uveřejňování dle tohoto článku je objednateli uložena § 219 ZZVZ.

4. Uveřejňování bude prováděno dle ZZVZ a příslušného prováděcího předpisu k ZZVZ.

Článek XIII
Ostatní ujednání

1. Poskytovatel prohlašuje, že je ke dni uzavření této smlouvy pojištěn pro případ vzniku odpovědnosti za škodu způsobenou v souvislosti s plněním této smlouvy, a to s horní hranicí pojistného plnění nejméně ve výši 2 000 000 Kč (slovy: dva miliony korun českých). Poskytovatel se zavazuje zajistit, že pojistná smlouva zůstane v uvedeném rozsahu platná a účinná po celou dobu trvání této smlouvy. Na výzvu objednatele je poskytovatel povinen kdykoliv v průběhu trvání smlouvy tuto skutečnost prokázat, a to do 5 pracovních dnů od doručení výzvy.

2. Smluvní strany se zavazují uzavřít písemný dodatek k této smlouvě, jehož předmětem bude úprava a doplnění práv a povinností smluvních stran vyplývajících z nově připravovaného zákona o kybernetické bezpečnosti, vyhlášky o kybernetické bezpečnosti nebo doprovodného zákona, a to vždy bez zbytečného odkladu poté, co předmětný právní předpis nebo jeho část nabyde platnosti.
3. Použije-li poskytovatel při své činnosti poddodavatele, nahradí škodu jím způsobenou, jakoby ji způsobil sám.
4. Poskytovatel je povinen:
   a) V souladu s ust. § 105 odst. 3 ZZVZ poskytnout objednateli identifikační údaje všech poddodavatelů, kteří nebyli identifikováni dle věty první uvedené v § 105 odst. 3 ZZVZ a kteří se následně zapojí do plnění předmětu dle této smlouvy, a to nejpozději před zahájením plnění předmětu dle této smlouvy poddodavatelem.
   b) Mít po celou dobu účinnosti této smlouvy platnou certifikaci ISO/IEC 27001:2022 či jinou rovnocennou certifikaci, kterou objednatel požadoval jako zadávací podmínku v zadávací dokumentaci zadávacího řízení, které předcházelo uzavření této smlouvy. Poskytovatel je povinen kdykoliv po dobu účinnosti této smlouvy na požádání objednateli tuto skutečnost doložit, a to přeložením příslušného platného certifikátu do 5 pracovních dnů ode dne doručení požadavku objednatele.
   c) V případě poskytování služeb prostřednictvím poddodavatele platí všechna ustanovení tohoto článku také pro poddodavatele a jeho pracovníky, kteří se budou na plnění smlouvy podílet. V případě, že poskytovatel splnil některý z kvalifikačních požadavků stanovených objednavatelem v zadávací dokumentaci zadávacího řízení, které předcházelo uzavření této smlouvy, prostřednictvím poddodavatele, je povinen v případě změny tohoto poddodavatele požádat objednatele o souhlas a prokázat, že nový poddodavatel tento kvalifikační požadavek splňuje, a to přede dnem zahájení poskytování plnění dle této smlouvy poddodavatelem. Odsouhlasení změny poddodavatele bude provedeno e-mailem alespoň jednou pověřenou osobou objednatele, bez povinnosti uzavřít dodatek k této smlouvě.
   d) Za plnění poskytovaná poddodavatelem je poskytovatel odpovědný jako by toto plnění poskytoval sám. Poskytovatel se zavazuje, že poskytne objednateli, pokud bude i část plnění poskytována poddodavatelem, seznam kontaktních údajů na osoby provádějící plnění za poddodavatele. Objednatel je oprávněn průběh plnění realizovaný poddodavatelem řešit napřímo s jeho pracovníky a poskytovatel není oprávněn tuto komunikaci s poddodavatelem či jeho pracovníky jakkoliv omezovat nebo mařit.

   Při porušení kterékoliv povinnosti objednatele podle písm. a) až d) tohoto odstavce je objednatel oprávněn od smlouvy odstoupit nebo ji vypovědět podle čl. XI odst. 4 písm. e).
5. Poskytovatel se zavazuje, že nebude využívat plnění pro objednatele (resp. označení České národní banky) jako veřejně dostupnou referenci bez předchozího písemného souhlasu objednatele.

Článek XIV
Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem jejího podpisu oprávněnými zástupci obou smluvních stran.
2. Smlouvu je možno měnit nebo doplňovat pouze formou písemných, vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran, není-li ve smlouvě

uvedeno jinak. Dodatek v elektronické podobě se považuje za řádně podepsaný objednatelem, je-li podepsán kvalifikovanými elektronickými podpisy.

3. Závazkový vztah založený touto smlouvou se řídí českým právním řádem, zejména občanským zákoníkem.
4. Spory vyplývající z této smlouvy budou řešeny především dohodou smluvních stran. Nebude-li možné dosáhnout dohody, bude spor řešen před místně a věcně příslušným soudem České republiky, a to výlučně podle českého práva.
5. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém nebo slovenském jazyce, nebude-li pověřenými osobami smluvních stran v konkrétním případě dohodnuto jinak.
6. Odpověď stran této smlouvy podle § 1740 odst. 3 občanského zákoníku s dodatkem nebo odchylkou není přijetím nabídky, ani když podstatně nemění podmínky nabídky.
7. Smluvní strany vylučují uplatnění ustanovení § 1765 a § 1766 občanského zákoníku na svůj smluvní vztah založený touto smlouvou, čímž se ruší nárok dodavatele na jednání podle § 1765 odst. 1 občanského zákoníku. Dodavatel tímto přebírá nebezpečí změny okolností dle § 1765 odst. 2 občanského zákoníku.
8. Práva a povinnosti vzniklé z této smlouvy mohou být postoupeny pouze po předchozím písemném souhlasu druhé smluvní strany.
9. V případě rozporu mezi některými ustanoveními smlouvy a jejími přílohami se smluvní strany dohodly na tom, že přednost má nejprve příloha č. 2, poté tělo smlouvy.
10. Ukončením smlouvy nejsou dotčena ustanovení smlouvy týkající se nároků z odpovědnosti za vady, nároků z odpovědnosti za škodu a nároků ze smluvních pokut, závazku mlčenlivosti ani další ustanovení, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti smlouvy.

11. Smlouva je vyhotovena v elektronické podobě, přičemž každá ze smluvních stran obdrží vyhotovení smlouvy opatřené elektronickými podpisy.

Přílohy:	Příloha č. 1	Podrobný popis parametrů služby
	Příloha č. 2	Technické požadavky objednatele
	Příloha č. 3	Bezpečnostní požadavky objednatele
	Příloha č. 4	Ujednání o zpracování osobních údajů
	Příloha č. 5 část A	Popis systémového prostředí objednatele (veřejná část)
	Příloha č. 5 část B	Popis systémového prostředí objednatele (neveřejná část)
	Příloha č. 6	Realizační studie ***(volně připojená příloha)***
	Příloha č. 7	Obecná pravidla pro poskytovatele
	Příloha č. 8	Šablona realizační studie

V Praze

Za objednatele:

[redacted]

Ing. Milan Zirnsák
ředitel sekce informatiky
podepsáno elektronicky

[redacted]

Ing. Zdeněk Virius
ředitel sekce správní
podepsáno elektronicky

V Praze

Za poskytovatele:

[redacted]

Ing. Jiří Buneš
na základě pověření
podepsáno elektronicky

[redacted]

Příloha č. 1

Podrobný popis parametrů služby

Popis Služby

Předmětem Služby je automatická detekce kybernetických bezpečnostních událostí zajištěná korelací dat získaných z prvků IT infrastruktury Zadavatele.

Primárně jsou zpracovávána data ve formě logů, přičemž je podporován sběr a zpracování logů ze standardních i nestandardních zdrojů - fyzická či virtuální zařízení Zadavatele (dále jen „Systémy“) vybraných výrobců podporovaných výrobcem SIEM. Sekundárně jsou využívána kontextová data (např. CMDB, IDM, manuálně plněné seznamy apod.) Logy i další zpracovávaná data jsou dále souhrnně označována jen jako „logy“.

Všechny identifikované bezpečnostní události jsou evidovány v multitenantním ticketovacím nástroji dohledového centra SOC Poskytovatele v samostatném tenantu, kde probíhá také jejich klasifikace, analýza a vyhodnocování. Události, které jsou vyhodnoceny jako podezření na bezpečnostní incident, jsou nahlášeny Zadavateli. Veškeré činnosti jsou technicky i procesně v souladu s požadavky směrnic řady ISO 27000.

I.1 Charakteristika Služby

1) Služba je poskytována technickými prostředky na straně Zadavatele.
2) V prostředí Zadavatele jsou umístěny stávající kolektor servery pro sběr a zabezpečený přenos logů ze Systémů do SIEMu a rovněž na úložiště dat.
3) Zadavatel disponuje vlastní rozsáhlou databází detekčních metod, které jsou kontinuálně rozvíjeny.
4) V SIEMu jsou logy zpracovány na základě detekčních pravidel a identifikované bezpečnostní události (alerty) jsou automaticky postoupeny prostřednictvím online ticketovacího nástroje ke zpracování SOC analytikům Poskytovatele.
5) SOC určí, zda je událost true/false positive, a u true positive vyhodnotí závažnost události. Je-li bezpečnostní událost vyhodnocena jako validní (oklasifikována stupněm závažnosti „Vysoký“, „Střední“ nebo „Nízký“), založí SOC upozornění a doplní doporučení k řešení bezpečnostní události, které předá Zadavateli dle postupu stanoveného v komunikační matici. Zadavatel následně zajistí prověření události ve svém IT prostředí a má možnost zaznamenat zpětnou vazbu nebo požádat o součinnost SOCu.
6) Bezpečnostní události Zadavatele jsou evidovány dohodnutým způsobem např. v zákaznickém webovém portálu Služby (dále jen „Portál“), kde probíhá rovněž:
    a. agregace událostí na základě klíčových atributů
    b. evidence životního cyklu bezpečnostní události (vyhodnocování, eskalace, způsob řešení).

7) Portál je dále využíván pro:
    a. reporting,
    b. volitelně - zobrazení aktuálního stavu zpracování bezpečnostních událostí (dashboardy),
    c. evidenci požadavků Smluvního partnera ke změně Služby (dále jen „Pokyn“),

d. monitoring SLA Služby.

8) Činnosti dohledového centra SOC

a. Služby dohledového centra SOC jsou poskytovány v režimu 24x7 a dle smluvně stanoveného SLA

b. Analytická činnost (triáž a klasifikace bezpečnostních událostí)

c. Návrhy řešení bezpečnostních událostí

d. Návrhy technických a organizačních opatření

e. Hlášení bezpečnostních událostí Zadavateli dle definovaného procesu.

f. Provozní monitoring všech technických součástí Služby spravovaných Poskytovatelem.

g. Měsíční reporting pro Zadavatele, dle požadované specifikace.

I.2 Technická specifikace Služby

V rámci Služby je standardně zajištěn monitoring Systémů podporovaných použitým SIEM nástrojem. Seznam aktuálně podporovaných Systémů v rámci SIEM nástroje je k dispozici u Poskytovatele na vyžádání.

I.2.1 Portál

1) Portál může Smluvní partner využít zejména
   - ke zpracování bezpečnostních událostí,
   - k odběru měsíčních reportů,
   - k přístupu do technické a provozní dokumentace Služby, která je vlastnictvím Poskytovatele a k níž Poskytovatel drží majetková práva autorská.
2) Přístup Smluvního partnera k Portálu je možný přes internet pomocí internetového prohlížeče. Přístup je umožněn po ověření uživatele na straně Smluvního partnera pomocí přístupového ID, hesla a uživatelského certifikátu.
3) Smluvní partner obdrží až pět personalizovaných účtů pro přístup do Portálu.
4) V přehledovém panelu („dashboardu“) Portálu Zadavatel může vidět přehled alertů ze SIEMu. A FlowMonu. Zobrazené informace si Smluvní partner může také vyexportovat z Portálu pro další zpracování. Informace exportované z Portálu ani jejich jednotlivé části nejsou veřejným dokumentem sloužícím k prokazování skutečností v rámci soudních, správních, rozhodčích či jiných řízení a nemají povahu znaleckého posudku ani jiného obdobného dokumentu, přičemž bez souhlasu Poskytovatele není Smluvní partner oprávněn je tímto způsobem použít.
5) Smluvní partner má možnost podávat dotazy ke Službě prostřednictvím Portálu. Reakce Poskytovatele na tyto dotazy ani hlášení nepodléhá SLA.
6) Kontaktní osoby Smluvního partnera pro Službu

   ADSR uvedený ve Specifikaci služby

   a. může provést změnu Specifikace služby

   b. ADSR nemůže bez dalšího oprávnění přistupovat na Portál a dávat Poskytovateli Pokyny k úpravě Služby

   Kontaktní osoba

   a. může přistupovat na Portál a dávat Poskytovateli jeho prostřednictvím všechny typy Pokynů

I.3 Zavedení a změna Služby

Na základě požadavku zadávací dokumentace bude realizace rozdělena do 3 etap.

Etapa 1 – Realizační studie
V této etapě bude na základě společných workshopů podrobně zmapován aktuální stav a vydefinovány nutné prerekvizity pro fungování služby (komunikační matice, nakládání s osobními údaji, struktura a obsah měsíčního reportu, atd.). Nejdůležitější částí této etapy bude podrobné prozkoumání stávajících korelačních pravidel a analýza aktuálních zdrojů logů. Výsledkem bude podrobný rozpad veškerých korelačních pravidel a návrhy / doporučení, jak tato pravidla upravit / smazat včetně návrhu časového harmonogramu. Zároveň bude vytvořen seznam zdrojů logů a případné doporučení na rozšíření nebo úpravu stávajících zdrojů. Na základě zjištěných údajů bude vytvořen dokument Realizační studie, kde budou sepsána veškerá doporučení a navrhované změny. Etapa bude ukončena akceptací Realizační studie.

Etapa 2 – Implementace
Tato etapa bude zaměřena na zavedení navržených změn v Realizační studii. Vzhledem k již existujícímu kontraktu mezi Zadavatelem a poskytovatelem jsou již nastavena přístupová práva Poskytovatele do prostředí Zadavatele (VPN, certifikáty, přístupy do systémů, apod.), a proběhne jejich revize a aktualizace. Nejdůležitějším bodem je úprava stávajících korelačních pravidel. Úprava těchto pravidel bude podléhat připravenému harmonogramu v Realizační studii. Díky aktualizaci stávajících pravidel, případně přidáním nových či odstranění redundantních, dojde k optimálnímu fungování a minimalizaci falešně pozitivních událostí. Dále je již poskytován nepřetržitý (24x7) monitoring bezpečnostních událostí s využitím systému SIEM a FlowMon Zadavatele, včetně následného vyhodnocování.

Etapa 3 – Ověřovací provoz
V této etapě již probíhá běžný provoz a nutné ladění korelačních pravidel, reportingu a auditních politik na dohlížených systémech tak, aby odpovídaly očekávání Zadavatele. Po ukončení tohoto ověřovacího provozu dojde k jeho akceptaci Zadavatelem a následnému překlopení do běžného provozu. V případě výhrad budou navržena a následně implementována nápravná opatření.

Příloha č. 2

Technické požadavky objednatele

Níže jsou uvedeny základní věcné funkční požadavky na poptávanou službu SOC. Z pohledu objednatele se jedná o nejdůležitější požadavky, které mají umožnit splnění cíle uvedeného v preambuli této smlouvy.

U každého požadavku je uveden jak jeho název a definice dle objednatele, tak i popis tohoto požadavku. Dále jsou pak případně uvedeny konkrétní komponenty či produkty, které by dle objednatele umožňovaly splnění daných požadavků.

U všech požadavků se jedná o závazné požadavky.

1. Definice, akronymy a zkratky

Zkratka/Termín	Popis/Definice
Alert	Emailová notifikace systému SIEM, která informuje o podezření na detekovanou KBU/KBI.
KBU	Kybernetická bezpečnostní 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. KBI vzniká po analýze pouze z některých KBU.
SOC	Security operations center zajišťující monitoring bezpečnostních událostí, jejich analýzu a návrh protiopatření k detekovaným událostem. V případě ČNB externí SOC neobsahuje reakční složku, tu stále zajišťuje ČNB.
SIEM	Security Information and Event Management. Management bezpečnostních informací a událostí, jejich monitoring a vyhodnocování.
FlowMon	Systém pro monitoring síťového provozu a detekci anomálií.
Citrix ShareFile	Systém pro sdílení a přenos souborů.
Analýza	Jedná se o dohledání všech souvisejících informací k detekované KBU/KBI s pomocí systému SIEM a FlowMon, aby bylo možné rozhodnout, zda se jedná o False-positive alert, KBU, KBI, případně je nutné provést místní šetření.

2. Požadavky na monitoring a analýzu bezpečnostních událostí

a) Poskytovatel provádí nepřetržitý vzdálený dohled/monitoring bezpečnostních událostí s využitím systému SIEM objednatele, a to 24 hodin denně 7 dnů v týdnu po celý rok.
b) Poskytovatel provádí proaktivní vyhledávání a analýzu potencionálních KBU v pracovních dnech na základě znalostí o nových typech útoků a znalosti systémového prostředí ČNB, případně jiných podezřelých bezpečnostních událostí, které SIEM nedetekuje nebo negeneruje alert.

c) Poskytovatel provádí proaktivní vyhledávání konfiguračních chyb z bezpečnostních logů monitorovaných systémů, a to v minimálním rozsahu 1 hodiny týdně.
Jedná se o chyby, které mohou mít vliv na provoz nebo bezpečnost IT/IS, mnohačetné nebo pravidelně se opakující.
d) Poskytovatel provádí detailní analýzu KBU dle operativně zaslaného požadavku osobou k tomu oprávněnou dle komunikační matice (viz příloha č. 6). Poskytovatel do 2 hodin od zaslání požadavku rozhodne, zda se jedná o KBU/KBI, a informuje o výsledku objednatele; konkrétní způsob informování je uveden v komunikační matici (viz příloha č. 6).
Jedná-li se o KBU/KBI, postupuje se dále podle bodu h) až k).
Nejedná-li se o KBU/KBI, bude vypracována písemná analýza, která musí obsahovat kromě běžných identifikačních údajů zejména všechny souvisejících informace ze systému SIEM a FlowMon, případně veřejných informací dostupných na internetu pro detailní objasnění vzniklé události v zaslaném požadavku. Analýza bude objednateli postoupena v souladu s komunikační maticí (viz příloha č. 6).
e) Poskytovatel poskytne analytickou pomoc v případě potvrzeného kybernetického útoku, včetně pomoci při zajišťování auditní stopy pro následnou analýzu.
f) Poskytovatel vylepšuje bezpečnostní monitoring systému SIEM objednatele (pravidla, reporty, aletry apod.), a to vytvářením kontentu v SIEM objednatele, nebo formou balíčků pro nástroj ArcSight, aby byl schopen garantovat vysokou kvalitu dodávané služby.
Nová pravidla nebo úpravy stávajících navrhuje zejména na základě proaktivního vyhledávání KBU dle bodu b), výsledků analýzy dle bodu d) a e) nebo svých zkušeností. Implementaci vytvořených pravidel provádí objednatel.
Všechny související činnosti potřebné pro úplnou analýzu (instrukce pro zaměstnance poskytovatele, playbooky apod.) zajišťuje poskytovatel.
g) Poskytovatel vyhodnocuje alerty detekované systémem SIEM objednatele, popř. KBU/KBI přímo takto označené systémem SIEM, do 2 hodin od jejich detekce, tj. okamžiku zobrazení alertu v seznamu v konzoli SIEMu, bez ohledu na to, zda a kdy došlo k zaslání nebo doručení avíza ze systému SIEM objednatele e-mailem poskytovateli.
h) Do doby dle bodu g) rozhoduje poskytovatel o tom, zda se z alertu stává KBU nebo KBI v definované kategorii, či se jedná o „false positive“ alert, kterým se již obě smluvní strany dále nezabývají, a výsledek analýzy odešle objednateli. Pokud nelze jednoznačně rozhodnout, zda se jedná o „false positive“ alert, vypracuje poskytovatel detailní podklady všech souvisejících informací ze systému SIEM a FlowMon, včetně ohodnocení předpokládané závažnosti, a předá je objednateli. Objednatel si může vyžádat další analýzu a doplnění podkladů.
    a. Při vyhodnocování závažnosti KBU/KBI poskytovatel zohledňuje důležitost jednotlivých technických aktiv (serverů, aktivních prvků, stanic, databází…), tj. klasifikaci provozovaných informačních systémů podle zákona o kybernetické bezpečnosti.
    b. V případě vyhodnocení detekované události jako KBU provede poskytovatel její analýzu, o jejímž výsledku informuje objednatele.
    c. V případě vyhodnocení detekované události jako KBI, nebo v případě podezření na KBI, nebo pokud není jednoznačné, že se nejedná o KBI, odešle poskytovatel objednateli zprávu a pokračuje dále v analýze. O nově zjištěných podstatných skutečnostech neprodleně informuje objednatele.
i) Během analýzy KBU/KBI i po jejím ukončení poskytovatel informuje objednatele v souladu s komunikační maticí o opatřeních, která je potřeba udělat v informačních systémech objednatele, aby se zamezilo útoku a minimalizovaly škody.
j) Analýza musí obsahovat všechny souvisejících informace k detekované KBU/KBI ze systému SIEM a FlowMon, případně veřejných informací dostupných na internetu.

k) Pokud objednatel usoudí, že informace z provedené analýzy nejsou dostačující, může si vyžádat jejich doplnění. Analýza následného obdobného typu KBU/KBI již musí tyto informace obsahovat.
l) Poskytovatel musí garantovat vyhodnocení minimálně 100 událostí detekovaných systémem SIEM za kalendářní měsíc a 5 operativně zaslaných požadavků dle bodu d).
m) K analýze KBU, KBI nebo alertu využívá poskytovatel systém SIEM a FlowMon objednatele, případně informace dostupné z veřejných zdrojů.
n) Veškerá komunikace probíhá dle závažnosti KBI a komunikační matice. Výsledky analýzy, podklady k alertům a reporty jsou předávány elektronicky, přes sdílený prostor v systému Citrix ShareFile.

Pravidla pro určení závažnosti bezpečnostního incidentu (KBI)

Závažnost bezp. incidentu	Popis	Komunikace
Kritický	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 bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.	Telefonicky a e-mailem
Střední	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 incidentu včetně minimalizace vzniklých škod.	E-mailem a SMS
Nízký	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 bezpečnostního incidentu včetně minimalizace vzniklých škod.	E-mailem

3. Požadavky na pravidelný měsíční report

a) Poskytovatel odešle objednateli do 5. pracovního dne v měsíci report s informacemi za předchozí měsíc.
b) Report bude obsahovat minimálně:
   - statistiku sbíraných událostí a typů zdrojů těchto událostí,
   - statistiku korelovaných událostí prostřednictvím ArcSight ESM (Enterprise Security Manager),
   - statistiku o úspěšných/neúspěšných přihlášeních uživatelů,
   - anomálie v počtu sbíraných logů dle jednotlivých zdrojů,
   - TOP nestandardně komunikujících zařízení dle zdrojové/cílové adresy,
   - TOP detekujících ADS (Anomaly Detection Systém) metod (FlowMon),
   - TOP ADS alertů za zařízení (FlowMon),

- seznam alertů ze systému SIEM objednatele analyzovaných poskytovatelem,
- seznam a způsob řešení zjištěných incidentů (KBU/KBI),
- seznam nalezených bezpečnostních a provozních problémů (Hunting) vč. konfiguračních chyb z bezpečnostních logů monitorovaných systémů – u těch bude potvrzena i časová dotace 3 hodiny týdně,
- seznam relevantních nových hrozeb s možným dopadem na aktuálně používaná aktiva ČNB, o kterých se poskytovatel dozvěděl, se stručným popisem, případně odkazem na podrobnosti, pokud je k dispozici,
- seznam provedených úprav SIEM (pravidla, reporty apod.) včetně podrobného popisu,
- návrh na nastavení sběru logů z nových zdrojů nebo úpravy stávajících, které jsou pro detekci KBU významné, vlastní sběr nebo úpravy zajistí objednatel,
- počet skutečně odpracovaných hodin plnění dle čl. I odst. 1 písm. j), včetně podrobného rozpisu.

4. Bezpečnostní požadavky

ID	Název	Popis požadavku
S1	Bezpečnost u subdodavatelů	Bezpečnostní požadavky na poskytovatele poskytovatel přenáší na subdodavatele jako součást smlouvy v rozsahu, který odpovídá charakteru dodávky.
S2	Certifikace řízení bezpečnosti	Poskytovatel má a udržuje po celou dobu plnění certifikovaný systém řízení bezpečnosti informací podle ISO/IEC 27001:2022 nebo ekvivalentní, v jehož rozsahu jsou služby poskytované objednateli a zařízení, která slouží k poskytování těchto služeb.
S3	Hlášení incidentu	Poskytovatel oznámí objednateli co nejdříve každé narušení bezpečnosti systémů poskytovatele, které způsobilo nebo by mohlo způsobit prozrazení informací, které získal od objednatele, nebo neoprávněný přístup k systémům objednatele. Při tom použije stejný způsob informování jako při detekování bezpečnostní incidentu kategorie kritický u objednatele.
S5	Poučení uživatelů	Pracovníky poskytovatele, kteří mají přístup k systémům a informacím objednatele, poskytovatel před umožněním takového přístupu prokazatelně poučí o jejich povinnostech k zajištění bezpečnosti a o bezpečnostních opatřeních. Objednatel si může vyžádat od poskytovatele provedení poučení o bezpečnosti IT v aktuální verzi a poskytovatel je povinen ho doložit do 1 měsíce od vyžádání.
S6	Smazání informací	Nejpozději při ukončení smluvního vztahu poskytovatel odstraní ze svých informačních systémů (případně zlikviduje tištěné materiály) informace o bezpečnostních událostech a incidentech, informačních systémech objednatele a jejich konfiguracích. Přitom dodrží požadavky přílohy 4 vyhlášky č. 82/2018 Sb.

Bezpečnostní požadavky na systém, ze kterého pracovníci poskytovatele přistupují k SIEM, případně k dalším systémům objednatele:

ID	Název	Popis požadavku
S10	Jednoznačný identifikátor uživatele	Každý uživatel má jednoznačný uživatelský účet. Sdílené účty (pokud jsou použity) jsou schváleny a dokumentovány a jejich použití monitorováno.
S11	Správa práv	Přidělování a odebírání přístupových práv uživatelským účtům se řídí dokumentovaným procesem. Přístupová práva jsou evidována.

ID	Název	Popis požadavku
S12	Řízení privilegovaných účtů	Uživatelské účty s privilegovaným oprávněním jsou schválené a dokumentované. Uživatelské účty s privilegovaným oprávněním jsou odlišné od uživatelských účtů. Uživatelské účty s privilegovaným oprávněním jsou pravidelně revidovány.
S13	Dočasná hesla	Dočasné tajné autentizační údaje (např. heslo) jsou předány uživatelům pouze po předchozí identifikaci uživatele, nesmí být uhodnutelné a musí být změněny po prvním použití.
S14	Defaultní účty	Defaultní účty jsou odstraněny nebo uzamčeny. Pokud to není možné, jsou změněny tajné autentizační údaje (např. hesla) k nim.
S15	Odebrání přístupu	Při ukončení pracovního poměru (nebo jiné smlouvy opravňující k přístupu) jsou uživateli odebrána všechna přístupová práva a deaktivován uživatelský účet.
S16	Autorizace	Před přístupem k datům a funkcím systému mimo těch, které jsou veřejné, je uživatel autentizován a je ověřen rozsah jeho oprávnění.
S17	Žádná nezměnitelná hesla	K žádné části systému není možné získat přístup s využitím autentizačních informací (hesel, kryptografických klíčů apod.), které není možné změnit. Tj. systém neobsahuje „hardcoded“ hesla, „maintenance backdooor“ apod.
S18	Bezpečná hesla	Používaná hesla musí splňovat požadavky zákona o kybernetické bezpečnosti č. 181/2014 Sb. a navazujících předpisů.
S19	Fyzická bezpečnost	Systémy mají zajištěnou fyzickou bezpečnost, tj. jsou chráněny před krádeží a přístupem neoprávněných osob.
S20	Likvidace médií	Média (flash disky, pevné disky atd.), na kterých byly uloženy informace získané od objednatele, jsou před dalším použitím bezpečně smazána. Po skončení životnosti jsou bezpečně zlikvidována.
S21	Logování	Systém zaznamenává informace o provozních a bezpečnostních činnostech. Tyto záznamy jsou chráněny proti pozdější modifikaci a neoprávněnému smazání.
S22	Synchronizace času	Čas na všech technických aktivech systému je synchronizován se zdrojem přesného času nejméně jednou za 24h.
S23	Pouze podporovaný software	Je provozovaný pouze dodavatelem podporovaný software nebo software s otevřeným kódem. (Není provozován software, který už není dodavatelem podporován.)
S24	Žádné modifikace software	Software dodaný výrobcem není před instalací modifikován.
S25	Instalace kritických aktualizací	Bezpečnostní aktualizace programového vybavení systému, které jeho výrobce označil jako kritické, jsou aplikovány do … dnů od vydání.
S26	Odstraňování zranitelností	Systém je pravidelně skenován na přítomnost známých zranitelností. Vysoce závažné zranitelnosti (Common Vulnerability Scoring System score 7 a vyšší, jsou odstraněny do 90 dnů. Není-li možné takovou zranitelnost v této lhůtě odstranit, poskytovatel o ní informuje objednatele.
S27	Ochrana před škodlivým kódem	Je zajištěna ochrana před škodlivým kódem, například nasazením pravidelně aktualizovaného antivirového programu prověřujícího spouštěné a otevírané soubory.
S28	Ochrana přenášených dat	Důvěrnost a integrita dat přenášených po sítích mimo prostory pod správou poskytovatele jsou chráněny kryptografickými opatřeními.
S29	Ochrana dat na médích	Důvěrnost a integrita dat ukládaných na vyměnitelná média a mobilní zařízení přenášené mimo prostory pod správou poskytovatele jsou zajištěny kryptografickými opatřeními.

ID	Název	Popis požadavku
S30	Bezpečná kryptografie	Použité kryptografické algoritmy, schémata a protokoly splňují požadavky zákona o kybernetické bezpečnosti č. 181/2014 Sb. a navazujících předpisů.
S31	Procesní zabezpečení VPN poskytovatelem	a) Poskytovatel si zajistí instalaci a konfiguraci aplikace Citrix Workspace a certifikátů na PC zaměstnanců SOC, dle návodu od objednatele. b) Poskytovatel nesmí mít na klientském zařízení aktivovanou funkci SSO (Single Sign-On), která by ovlivňovala autentizaci k publikovaným aplikacím objednatele. c) Poskytovatel zajistí uložení klíče od objednatele do registru operačního systému Windows na PC zaměstnanců SOC. d) Poskytovatel oznámí objednateli nástup nového zaměstnance SOC minimálně 5 pracovních dnů před požadavkem na vydání certifikátu objednatelem na adresu dle komunikační matice dohodnuté v rámci realizační studie. Certifikát je zaměstnanci vydán na jeho vlastní čipovou kartu/token v sídle objednatele v pracovní době ČNB. e) V případě obnovy certifikátu z důvodu vypršení certifikátu, chyby nebo ztráty bude zaměstnanci SOC vydán certifikát nový na jeho vlastní čipovou kartu/token v sídle objednatele v pracovní době ČNB. f) Maximální počet souběžně platných certifikátů všech zaměstnanců SOC je 15.
S32	Hlášení změny u osoby	Poskytovatel je povinen neprodleně oznámit objednateli rozvázání pracovního poměru se zaměstnancem SOC, změnu pracovního zařazení, případně ztrátu certifikátu, na jehož základě Objednatel zneplatní certifikát tohoto zaměstnance.
S33	Standard pro čipovou kartu či token poskytovatele	Poskytovatel v rámci karet či tokenů pro VPN si zajistí vlastní zařízení: Čipové karty od firmy Gemalto model IDPrime 940/B nebo usb tokeny CC 5110 (940)

Příloha č. 3

BEZPEČNOSTNÍ POŽADAVKY OBJEDNATELE

1. Poskytovatel odpovídá za to, že do objektů objednatele (dále jen „ČNB“) budou vstupovat nebo vjíždět pouze ti jeho pracovníci, kteří jsou jmenovitě uvedeni v seznamu pracovníků schváleném ČNB (dále jen „seznam“). Tato povinnost se vztahuje i na posádky vozidel poskytovatele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Poskytovatel předloží seznam ČNB nejpozději pět pracovních dní před zahájením prací.
2. Seznam bude obsahovat tyto položky: jméno, příjmení a číslo průkazu totožnosti každého z pracovníků poskytovatele. Poskytovatel se zavazuje zajistit, aby všichni jeho pracovníci uvedení v seznamu byli ještě před předložením seznamu ČNB proškoleni o podmínkách zpracování osobních údajů a o právech subjektů údajů ve smyslu obecného nařízení o ochraně osobních údajů - Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“). Poskytovatel se zejména zavazuje, že všichni jeho pracovníci uvedení v seznamu budou nejpozději do okamžiku předložení seznamu ČNB poučeni:
   a) o tom, že poskytovatel předá jejich osobní údaje v rozsahu: jméno, příjmení a číslo průkazu totožnosti České národní bance, sídlem Na Příkopě 28, Praha 1 v rámci plnění této smlouvy, a to za účelem ochrany práv a oprávněných zájmů ČNB (zajištění evidence osob vstupujících do budovy ČNB z důvodu ochrany majetku a osob a správy systému kontrol vstupů ČNB);
   b) o veškerých právech subjektu údajů, která mohou uplatnit vůči poskytovateli a ČNB, zejména o právu na přístup k osobním údajům, které jsou o nich zpracovávány, právu na námitku proti zpracování osobních údajů, právu požadovat nápravu situace, která je v rozporu s právními předpisy, a to zejména formou zastavení nakládání s osobními údaji, jejich opravou, doplněním či odstraněním, jakož i o právu podat stížnost k Úřadu pro ochranu osobních údajů.
3. Za poučení svých pracovníků ponese poskytovatel vůči ČNB následně odpovědnost. V případě nesplnění povinnosti podle odst. 2 této přílohy nahradí poskytovatel újmu, která v souvislosti s uvedeným ČNB vznikne, a to včetně případné nemajetkové újmy vzniklé poškozením dobrého jména a dobré pověsti, újmy vzniklé v důsledku postihu pravomocně uloženého ČNB správním nebo jiným k tomu oprávněným orgánem veřejné moci a újmy vzniklé ČNB v důsledku úspěšného uplatnění práv pracovníků poskytovatele vůči ČNB.
4. Požadavky na případné doplňky a změny schváleného seznamu je nutno neprodleně oznámit ČNB. Případné doplňky a změny seznamu podléhají schválení ČNB. Osoby neschválené ze strany ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.
5. Poskytovatel uvede předem ty své pracovníky, pro které požaduje vystavení vstupních karet ke vstupu do objektů ČNB. Vystavení vstupních karet podléhá schválení ze strany ČNB. První vstupní karty budou vystaveny na náklady ČNB. Každé další vystavení vstupní karty bude zpoplatněno částkou 200,- Kč (vč. DPH) s tím, že tato částka bude poskytovateli vyfakturována. Za vystavení nové vstupní karty nebude nutné platit v případech, kdy:
   - dosavadní karta přestane fungovat bez viditelného mechanického poškození,
   - dojde ke změně příjmení pracovníka,

- byla karta odcizena a událost je doložitelná protokolem od Policie ČR.

6. Poskytovatel bude při zahájení činnosti pro ČNB vybaven základním počtem vstupních karet pro jednotlivé pracovníky podle schváleného seznamu. Vstupní karta umožní oprávněnému pracovníkovi poskytovatele samostatný vstup do vyhrazených prostor objektu ČNB a samostatný pohyb v nich. Každá vstupní karta bude nepřenosná a bude vydávána odborem bankovní bezpečnosti a krizového řízení ČNB.
7. Vstupní karty budou vydávány ze strany ČNB pro každého pracovníka poskytovatele jednotlivě proti podpisu, a to po předložení výpisu z rejstříku trestů, který nebude starší než tři měsíce. Výpis z rejstříku trestů bude pracovníkovi vrácen. Při převzetí vstupní karty bude dotčený pracovník poskytovatele poučen o způsobu používání vstupní karty a o režimu vstupu osob a vjezdu vozidel do objektů ČNB a o pohybu v nich.
8. Pracovník poskytovatele, kterému byla vydána vstupní karta, je povinen okamžitě po zjištění ztráty, odcizení, zneužití, zničení nebo poškození vstupní karty, které brání jejímu řádnému užívání, toto oznámit odboru bankovní bezpečnosti a krizového řízení ČNB.
9. Při ukončení pracovního poměru pracovníka poskytovatele uvedeného v seznamu nebo při ukončení plnění podle smlouvy je poskytovatel povinen neprodleně vrátit vstupní kartu dotčeného pracovníka odboru bankovní bezpečnosti a krizového řízení ČNB.
10. ČNB si vyhrazuje právo nevydat vstupní karty pracovníkům poskytovatele bez udání důvodu.
11. ČNB si vyhrazuje právo vstupní kartu pracovníkovi poskytovatele odebrat z důvodu porušení režimu vstupu osob a vjezdu vozidel do objektu ČNB nebo porušení režimu pohybu v něm.
12. ČNB si vyhrazuje právo vyřadit i schválené pracovníky poskytovatele ze seznamu bez udání důvodů. Schválení pracovníci musí dodržovat směrnice ČNB a pokyny ostrahy pro vstup do vyhrazených prostor a pro pobyt v nich.
13. Pracovníci poskytovatele jsou povinni podrobit se při každém vstupu do objektu ČNB bezpečnostní kontrole prováděné bankovními policisty.
14. ČNB si vyhrazuje právo nevpustit do objektů ČNB pracovníka poskytovatele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.
15. Vstup do objektů ČNB se zvířaty je zakázán.
16. Vstup soukromých návštěv do vnitřních prostor objektů ČNB je zakázán. Pro tyto účely je možné využít určené návštěvní místnosti.
17. Poskytovatel a jeho pracovníci budou věnovat při plnění díla v oblasti požární ochrany zvýšenou pozornost:
    - dodržování právních předpisů o požární ochraně,
    - předpisům ČNB při provádění požárně nebezpečných prací se zvýšeným požárním nebezpečím (svařování, řezání plamenem, pájení, broušení, rozbrušování apod.),
    - průrazům a průchodům u rozvodů instalací a technologií hranicemi požárních úseků, včetně zachování, obnovení nebo nového vyhotovení jejich protipožárních ucpávek.
18. Poskytovatel se zavazuje zajistit, že jeho pracovníci, jakož i pracovníci případných jeho poddodavatelů, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se v průběhu plnění seznámí a které nejsou veřejně známy.

19. Povinnost mlčenlivosti podle odst. 19 této přílohy není časově omezena.
20. V případě mimořádné události se pracovníci poskytovatele musí řídit pokyny bankovních policistů nebo dozorujícího zaměstnance ČNB a dále instrukcemi vyhlašovanými vnitřním rozhlasem ČNB.
21. Pracovníci poskytovatele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny, hořlavé kapaliny, tlakové lahve apod. O tom, co je či není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.
22. Fotografování a pořizování videozáznamů je ve všech prostorách objektů ČNB zakázáno. Výjimku tvoří pořizování dokumentace technických havárií a poruch. Konkrétní případ musí předem písemně povolit ředitel odboru bankovní bezpečnosti a krizového řízení nebo ředitel příslušné pobočky ČNB.
23. Ve všech prostorách objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení k provedení požárně nebezpečné práce se zvýšeným požárním nebezpečím požádá poskytovatel písemnou formou dozorujícího zaměstnance ČNB, a to vždy nejpozději jeden pracovní den před zahájením prací.
24. Pracovníci poskytovatele se musí zdržet poškozování či odcizení majetku ČNB, a dále i jakéhokoli nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.
25. Pracovníci poskytovatele uvedení na seznamu se musí před započetím výkonu práce v objektech ČNB prokazatelně seznámit s „Pravidly pro smluvní partnery ČNB k zajištění bezpečnosti a ochrany zdraví při práci, požární ochrany a ochrany životního prostředí v ČNB“ (dále jen „pravidla“). Pravidla předá v listinné formě zástupci poskytovatele požární a bezpečnostní technik ČNB. Zástupce poskytovatele s pravidly seznámí všechny dotčené pracovníky poskytovatele.
26. ČNB je oprávněna v objektu ČNB kdykoliv podrobit kontrole kteréhokoliv pracovníka poskytovatele uvedeného na seznamu ohledně dodržování požární ochrany, bezpečnosti práce a všech výše uvedených ustanovení.

Příloha č. 4

Ujednání o zpracování osobních údajů
(dále také jen „***Ujednání***“)
(dodavatel nedoplňuje, bude doplněno před uzavřením ujednání)

Smluvní strany se dohodly na tomto Ujednání, které naplňuje požadavky stanovené pro smlouvu o zpracování osobních údajů podle ustanovení čl. 28 odst. 3 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 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 „***GDPR***“).

1. Úvodní ustanovení

1.1. Česká národní banka (dále též „***správce***“) v souladu **se smlouvou o poskytování služby SOC**, evidenční číslo smlouvy ČNB: _____ (dále jen „***smlouva***“) určuje účel a prostředky **zpracování osobních údajů zaměstnanců objednatele** (dále jen **„*interní uživatelé*“**) **a** _____ (dále jen **„*externí osoby*“**) (společně dále jen „***subjekty údajů***“) **a je tedy v postavení správce osobních údajů ve smyslu čl. 4 odst. 7 GDPR.**

1.2. _____ (dále též „***zpracovatel***“) bude na základě smlouvy zpracovávat osobní údaje subjektů údajů **a bude ve vztahu ke správci v postavení zpracovatele osobních údajů ve smyslu čl. 4 odst. 8 GDPR.**

2. Předmět Ujednání

Toto Ujednání upravuje vztahy mezi správcem a zpracovatelem a určuje jejich práva a povinnosti při zpracování osobních údajů zpracovatelem a v souvislosti s ním, zejména pak vymezuje rozsah osobních údajů, které bude zpracovatel zpracovávat, prostředky a účel, pro který bude osobní údaje zpracovávat, dobu zpracování osobních údajů, jakož i podmínky a záruky zpracovatele z hlediska technického a organizačního zabezpečení ochrany osobních údajů tak, aby zpracování probíhalo v souladu s právními předpisy v oblasti ochrany osobních údajů.

3. Účel zpracování a rozsah zpracovávaných osobních údajů

3.1. Zpracovatel bude zpracovávat osobní údaje subjektů údajů pouze v rozsahu nezbytném pro zajištění realizace smlouvy. Za osobní údaje jsou podle tohoto Ujednání považovány informace uvedené ve výčtu v odstavci 3.2 tohoto Ujednání („***osobní údaje***“).

3.2. Zpracovatel bude zpracovávat osobní údaje předané ze strany správce pro účely **zajištění služby podle čl. I odst. 1 smlouvy, provozu „security operation center“,** pouze v následujícím rozsahu nezbytném pro výkon práv a povinností podle smlouvy:

a) identifikační údaje;

b) identifikační číselné údaje;

c) síťové identifikátory.

3.3. Zpracovatel bude osobní údaje zpracovávat následujícími způsoby ve smyslu čl. 4 odst. 2 GDPR: nahlédnutím nebo jiným způsobem v souvislosti s účelem zpracování osobních údajů podle odstavce 3.2 tohoto Ujednání.

3.4. Zpracovatel je ve všech případech při zpracování osobních údajů vázán prokazatelnými pokyny správce. Zpracovatel nesmí bez předchozího prokazatelného výslovného souhlasu anebo pokynu správce zpracovávané osobní údaje upravit nebo pozměnit, třídit nebo kombinovat, zpřístupnit ani předat třetí osobě, šířit ani zveřejňovat, ani jakýmkoli způsobem použít pro vlastní potřebu.

4. Doba zpracování

4.1. Zpracovatel bude osobní údaje zpracovávat po dobu nezbytnou pro účel zajištění realizace smlouvy.

4.2. Po uplynutí doby zpracování podle odstavce 4.1 tohoto Ujednání bude zpracovatel osobní údaje zpracovávat v souladu s čl. 6 odst. 1 písm. c) a f) GDPR pouze v nezbytném rozsahu a výhradně za účelem plnění právními předpisy uložených povinností a ochrany práv a právem chráněných zájmů správce, zpracovatele, příjemce nebo jiné dotčené osoby, a to nejdéle po dobu vyplývající z příslušných zvláštních právních předpisů.

5. Práva a povinnosti smluvních stran

5.1. Správce pověřuje zpracovatele zpracováním osobních údajů výhradně za účelem podle odstavce 3.2 tohoto Ujednání.

5.2. Osobní údaje nebudou zpracovatelem zpracovávány ani s nimi nebude nakládáno jinak, než pouze za účelem, pro který byly osobní údaje zpracovateli poskytnuty, a vždy v souladu s pokyny správce; to platí i pro zpřístupnění či poskytnutí osobních údajů třetí osobě nebo předání mimo území EU.

5.3. Zpracovatel je povinen při každém případném využití cloudové služby předem informovat správce o tom, ve kterých zemích budou zpracovávané osobní údaje umístěny, a to i v případě jakékoli změny. Zařízení, na nichž budou osobní údaje uchovávány nebo jinak zpracovávány, se budou nacházet výlučně v zemích EU a osobní údaje budou předávány a uchovávány pouze v těchto zemích. Zpracovatel je zároveň povinen zajistit zpracování osobních údajů správce odděleně od případných osobních údajů jiných klientů zpracovatele.

5.4. Zpracovatel je povinen zabezpečit osobní údaje a zachovávat mlčenlivost o osobních údajích a řídit se pokyny správce ve všech případech, kdy se jedná o zpracování či zabezpečení osobních údajů. Zpracovatel přijme technická, organizační a personální opatření adekvátní způsobu zpracování a v souladu s pokyny správce – přičemž toto zabezpečení bude odpovídat příslušným aktuálním používaným bezpečnostním standardům (podrobněji v odstavci 5.5 a násl. tohoto Ujednání).

5.5. Správce stanoví opatření, která považuje za dostatečná pro technické a organizační zabezpečení osobních údajů následovně:

a) Technické zabezpečení osobních údajů bude zajištěno pomocí prostředků:

(i) **počítačové bezpečnosti**; zpracovatel se zavazuje ke zpracování používat výhradně takové technické a programové prostředky, jejichž používání při vyloučení nepředvídatelných okolností eliminuje možnost narušení, ztráty, zničení či poškození osobních údajů, neoprávněného přístupu k nim, či neoprávněného nakládání s osobními údaji;

(ii) **komunikační bezpečnosti**; zpracovatel se zavazuje dodržovat taková opatření k zabezpečení ochrany osobních údajů při jejich přenosu telekomunikačními kanály (včetně datových nosičů), jejichž povaha

eliminuje při vyloučení nepředvídatelných okolností možnost narušení (šifrování);

(iii) **fyzické bezpečnosti**; v tomto ohledu zpracovatel prohlašuje, že místo, ve kterém budou osobní údaje zpracovávány a ve kterém budou uchovávány spisy a dokumenty, bude mít charakter prostoru zabezpečeného před možností narušení bezpečnosti.

Zpracovatel bude plnit všechny povinnosti stanovené v tomto ustanovení písm. a) využíváním prostředků odpovídajících dosaženému stupni technického pokroku a nárokům odborné péče.

b) Organizační zabezpečení:

(i) osobní údaje budou zpřístupněny pouze určeným osobám z oprávněného personálu zpracovatele a případně oprávněným osobám, které odpovídají za zajištění bezpečnosti systému, kde jsou osobní údaje uloženy, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby;

(ii) zpracovatel je povinen zabezpečit poučení osob, které mají v rámci zpracování osobních údajů přístup k těmto údajům, aby všechny tyto osoby byly řádně poučeny o svých povinnostech při zpracovávání osobních údajů, zejména pak o povinnosti mlčenlivosti ve vztahu k těmto osobním údajům.

c) Dále je zpracovatel povinen:

(i) zabránit neoprávněným osobám v přístupu k osobním údajům a k prostředkům pro jejich zpracování, a také zabránit neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje.

5.6. Zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technická a organizační opatření k zajištění ochrany osobních údajů v souladu s právními předpisy, zejména s GDPR a dalšími předpisy v oblasti ochrany osobních údajů, jakož i provádět nejméně jednou ročně hodnocení efektivnosti přijatých opatření, a to včetně vedení a zpřístupnění následující dokumentace:

a) seznamu osob, které jsou oprávněny přistupovat k osobním údajům (včetně rozsahu oprávnění);

b) elektronického přehledu informací o veškerých přístupech jednotlivých osob k osobním údajům

c) elektronického přehledu informací o nakládání s osobními údaji.

5.7. Zpracovatel bude neprodleně písemně informovat správce v případě jakýchkoliv potíží při plnění povinností vyplývajících z tohoto Ujednání, jakož i o všech okolnostech týkajících se porušení povinností při zpracování a ochraně osobních údajů, zejména o případech, kdy dojde k náhodnému nebo protiprávnímu zničení, ztrátě či změně zpracovávaných osobních údajů nebo neoprávněnému poskytnutí nebo zpřístupnění zpracovávaných osobních údajů. V takovém případě zpracovatel přijme v nejkratším možném termínu veškerá nezbytná opatření k zajištění dostatečné ochrany osobních údajů, notifikuje správce o těchto skutečnostech prostřednictvím kontaktních osob uvedených ve smlouvě a následně postupuje v souladu s GDPR a pokyny správce, budou-li mu sděleny.

5.8. V případě, že v souvislosti se zpracováním osobních údajů zpracovatelem bude zahájeno řízení ze strany orgánu veřejné správy, zpracovatel poskytne správci v těchto řízeních veškerou potřebnou součinnost.

5.9. Zpracovatel je správci na jeho žádost nápomocen při posuzování vlivu zpracovávání osobních údajů na ochranu osobních údajů a při konzultacích správce s dozorovým orgánem, při zohlednění povahy zpracovávání a informací, jež má zpracovatel k dispozici.

5.10. Zpracovatel nezapojí do zpracovávání osobních údajů dalšího zpracovatele bez předchozího písemného povolení správce. V případě, že jakákoliv část zpracovávání osobních údajů bude vykonávaná dalším zpracovatelem po předchozím písemném povolení správce, zůstává zpracovatel plně odpovědný vůči správci za zpracovávání osobních údajů.

5.11. Správce je oprávněn kontrolovat dodržování pravidel stanovených pro zpracování v GDPR či v tomto Ujednání u zpracovatele, resp. i na jiném místě, kde dochází ke zpracování osobních údajů. Zpracovatel za tímto účelem zajistí zástupcům správce, kteří budou provedením kontroly pověřeni, přístup ke všem relevantním informacím a na všechna příslušná místa tak, aby mohlo být řádně provedeno hodnocení oprávněnosti zpracování. Zpracovatel poskytne správci na jeho vyžádání veškeré podklady o přijatých a provedených technických a organizačních opatřeních k zajištění ochrany osobních údajů.

5.12. Po ukončení poskytování služeb podle smlouvy zpracovatel neprodleně vrátí veškeré osobní údaje správci, s výjimkou údajů, které je zpracovatel povinen uchovávat na základě platných právních předpisů.

6. Odpovědnost za újmu a smluvní pokuty

6.1. Článek 6 upravuje odpovědnost za újmu a nárok na smluvní pokuty v případě porušení podmínek tohoto Ujednání. Znění tohoto článku 6 se nevztahuje na smluvní pokutu a úrok z prodlení podle článku X smlouvy, ve znění pozdějších dodatků, jehož platnost a účinnost zůstává v plném rozsahu zachována.

6.2. Zpracovatel se zavazuje nahradit správci jakoukoliv újmu, včetně nemajetkové, která vznikne z důvodu porušení tohoto Ujednání ze strany zpracovatele. V tomto závazku zpracovatele je zahrnuta i povinnost odškodnit správce za (i) jakékoliv nároky, a to zejména zadostiučinění, peněžité náhrady nebo pokuty, úspěšně uplatněné v soudním popř. správním řízení, ze strany třetích osob, (ii) za správní pokuty uložené správci pravomocně dozorovým orgánem, nebo (iii) jakoukoli újmu utrpěnou poškozením dobré pověsti v příčinné souvislosti s porušením povinností stanovených právními předpisy nebo tímto Ujednáním ze strany zpracovatele.

6.3. Pokud dojde k porušení GDPR nebo jiných právních předpisů v oblasti ochrany osobních údajů pouze v důsledku jednání té smluvní strany, které je v souvislsoti s tímto porušením uložena správní pokuta, hradí náklady na uhrazení správní pokuty plně ta strana, která GDPR nebo jiný právní předpis v oblasti ochrany osobních údajů prokazatelně porušila a jíž současně byla uložena pokuta.

6.4. V případě, že zpracovatel správci neumožní kontrolu ohlášenou v souladu s odstavcem 5.11 tohoto Ujednání, anebo během kontroly správci neposkytne pro předmět kontroly potřebnou součinnost, je správce oprávněn po zpracovateli požadovat smluvní pokutu ve výši 1 000 Kč za každý započatý pracovní den takto trvajícího prodlení na straně zpracovatele.

6.5. Zpracovatel je povinen odstranit kontrolou zjištěné nedostatky ve lhůtě 5 dnů, není-li mezi zpracovatelem a správcem dohodnuto jinak. V případě, že zpracovatel neodstraní kontrolou zjištěné nedostatky, je správce oprávněn po zpracovateli požadovat smluvní pokutu ve výši 1 000 Kč za každý započatý den prodlení na straně zpracovatele.

6.6. V případě, že zpracovatel poruší kteroukoli z povinností sjednaných v čl. 5 (vyjma odstavce 5.11) tohoto Ujednání, je správce oprávněn po zpracovateli požadovat smluvní pokutu ve výši 5 000 Kč za každý jednotlivý případ takového porušení.

6.7. Ujednáním o smluvní pokutě podle tohoto článku není dotčeno právo správce na náhradu škody vzniklé z porušení povinnosti.

6.8. Zpracovatel prohlašuje, že má platně uzavřeno pojištění v dostatečném rozsahu pro případ škody vzniklé porušením jeho povinností z tohoto Ujednání, a bude jej udržovat po celou dobu trvání závazků z tohoto Ujednání.

7. Trvání závazků

7.1. Závazek ke zpracování osobních údajů se sjednává pouze na dobu existence závazkového vztahu vzniklého ze smlouvy, nejpozději do dne likvidace posledního zpracovávaného osobního údaje zpracovatelem ve smyslu povinnosti zlikvidovat osobní údaje podle příslušných ustanovení GDPR.

7.2. V případě ukončení smlouvy předá zpracovatel veškeré osobní údaje správci na dohodnutém datovém nosiči a následně neprodleně zlikviduje veškeré záznamy (s výjimkou upravenou v odstavci 4.2 tohoto Ujednání) v jím spravovaných datových úložištích a na datových nosičích, včetně provozně-bezpečnostních záloh zpracovatele i datových záloh uložených u jeho případného poddodavatele

8. Další ujednání

8.1. Smluvní strany se zavazují vstoupit v jednání o doplnění tohoto Ujednání, pokud vyjde najevo potřeba takového doplnění zejména s ohledem na nově přijaté právní předpisy, stanoviska dozorových orgánů, nebo rozhodování soudních či správních orgánů, a poskytnout si veškerou potřebnou součinnost ke sjednání dodatku smlouvy, pokud bude pro potřeby plnění požadavků obecného nařízení či jiných právních předpisů potřebný.

8.2 Za písemnou formu se pro účely tohoto Ujednání nepovažuje e-mailová ani jiná elektronická forma. Výjimkou je situace, v níž zpracovatel informuje správce ve smyslu odstavce 5.7 (potíže při plnění povinností vyplývajících z tohoto Ujednání a okolnosti týkající se porušení povinností při zpracování a ochraně osobních údajů), a také oznámení kontroly ve smyslu odstavce 5.11, které lze provést i elektronickým oznámením prokazatelně doručeným druhé smluvní straně. V případě oznámení kontroly postačuje prokazatelné odeslání oznámení správcem na e-mailovou adresu _____ určenou pro tento účel zpracovatelem.

Příloha č. 5 část A

Popis systémového prostředí objednatele

1. Systém SIEM objednatele

1.1. konfigurace SIEM systému

Položka	Popis
Název	ArcSight ESM (plánován upg na ArcSight Recon a Detect)
Verze	7.4
Moduly	Konektory 8.4.x (cca. 50, instalovány na 3 serverech)
Licence	Denní průměr 1000 EPS (plánováno navýšení na 1500 EPS)

Do SIEM systému jsou posílány logy z cca 2000 datových zdrojů. Systém je zaměřen zejména (cca 2/3 všech datových zdrojů) na sběr logů aplikačních serverů, jejich databází a frontendů.
Vstupní logy jsou tvořeny událostmi z běžně používaných informačních technologií a systémů a událostmi ve specifickém formátu z unikátních aplikací zadavatele. Na první typ událostí jsou aplikovány parsery a pravidla ze standardní výbavy ArcSight, dodaná výrobcem. Pro druhý typ událostí jsou připraveny parsery na míru.
Množství logů produkovaných jednotlivými systémy kolísá podle aktivity uživatelů.

1.2. Statistika sběru dat do SIEM systému ČNB

Parametr	Hodnota	Předpokládaný počet pro následující období
Denní průměr EPS	950	1400
Maximum EPS	cca 800 (ve špičkách >2500)	1200 (ve špičkách >4000)
Minima EPS	300-350	500
Počet bezpečnostních událostí nahlášených SIEM systémem (za posledních 12 měsíců)	500	1000

EPS = počet událostí za vteřinu

2. Systém Flowmon objednatele

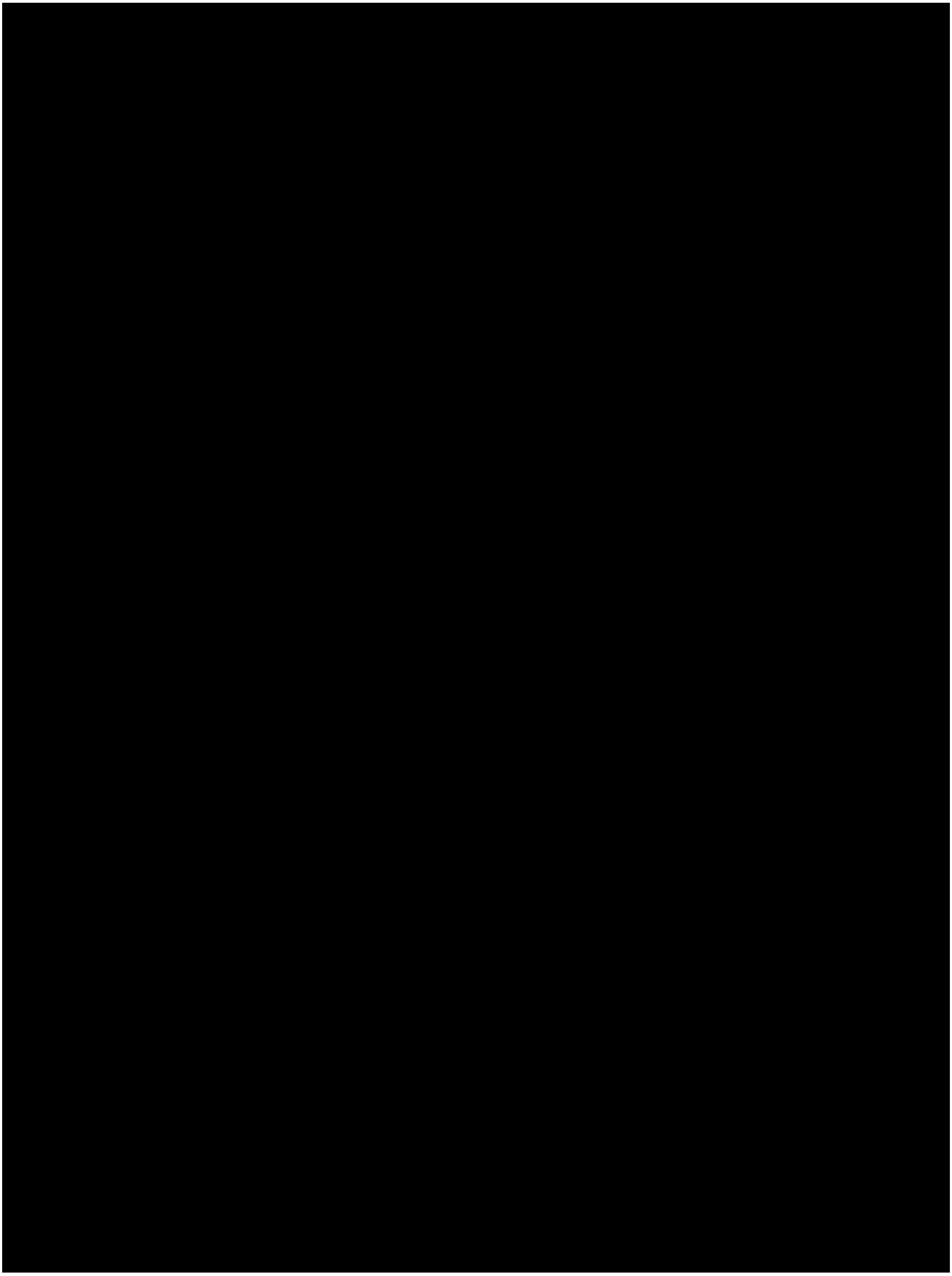
2.1. konfigurace Flowmon systému

Položka	Popis
Název	Flowmon (v roce 2024 bude vypsáno výběrové řízení na upgrade nebo náhradu jiným systémem pro analýzu bezpečnosti síťové komunikace)
Verze	12.02.04
Moduly	Monitoring Center, ADS

Položka	Popis
Licence	Flowmon Collector, ADS Corporate (obě licence ve verzi Gold Support výrobce)

Systém je tvořen jedním centrálním kolektorem a dvěma HW sondami. Dále jsou do kolektoru exportována NetFlow data z centrálních přepínačů, firewallů a wireless controllerů. Objem přijímaných toků osciluje dle denní doby okolo 2500 toků/s.

Příloha č. 5 část B



Příloha č. 5 část A (pokračování)

4. Popis vzdáleného přístupu (VPN)

4.1. Technická realizace

Vzdálený přístup prostřednictvím VPN je realizován pomocí produktů platformy CITRIX, konkrétně se jedná o publikované aplikace (konzole SIEM a FlowMon) prostřednictvím Citrix XenApp provozovaném na MS Windows Serveru 2016 s aktuálními SP a záplatami.

Na perimetru ČNB je instalována Citrix Access Gateway (Netscaler), který slouží jako bezpečný vstupní bod mezi klientským zařízením, objednatele, který používá pro zobrazení konzole SIEM a FlowMon objednatele.

Tento vstupní bod zajišťuje:

- Šifrovaný komunikační kanál mezi ČNB a poskytovatelem
- Prostřednictvím EPA agenta kontrolu bezpečnostní kvality koncového zařízení poskytovatele (aktuálnost patchů, antivirové ochrany apod.).
- Ověřovací bod pro přihlášení uživatelů poskytovatele.

Na klientském zařízení poskytovatele musí být nainstalována aplikace Citrix Workspace a nakonfigurována dle návodu od objednatele a nesmí být aktivována funkce SSO (Single Sign-On), která by ovlivňovala autentizaci k publikovaným aplikacím objednatele.

K přihlášení pracovníka poskytovatele se využívá dvoufaktorová autentizace – certifikát uložený na čipové kartě nebo tokenu aktivovaný PINem.

Při vytváření VPN spojení je nejprve provedena kontrola bezpečnostních prvků klientského zařízení a poté je uživatel připojen na publikované konzole SIEM a FlowMon.

Příloha č. 7

Obecná pravidla pro poskytovatele v oblasti bezpečnosti IT

1) Pokud jsou tato obecná pravidla v rozporu s ustanovením textu smlouvy/objednávky uzavírané mezi poskytovatelem a Českou národní bankou (dále jen „ČNB“) nebo textu zadávací dokumentace na veřejnou zakázku nebo jejich jinou přílohou, má přednost ustanovení textu smlouvy/objednávky nebo zadávací dokumentace nebo jejich jiná příloha.
2) Poskytovatel je povinen zajistit, že jeho pracovníci či poddodavatelé a jejich pracovníci, kteří se budou na plnění podle smlouvy/objednávky podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u ČNB seznámí a které nejsou veřejně dostupné. Povinnost mlčenlivosti není časově omezena.
3) Poskytovatel je rovněž povinen chránit informace, které nejsou veřejně dostupné, zejména předanou dokumentaci, před jejich prozrazením a/nebo zpřístupněním neoprávněným osobám a dále použít získané informace výhradně pro účely plnění smlouvy/objednávky s ČNB.
4) Poskytovatel nemá vzdálený přístup k systémům a do počítačové sítě ČNB.
5) Pracovníci poskytovatele, kteří budou samostatně přistupovat k informačním systémům a systémovému prostředí ČNB, se před nebo při prvním přístupu musí seznámit s bezpečnostními požadavky a svými povinnostmi vyplývajícími z vnitřních předpisů ČNB.
6) Poskytovatel a jeho pracovníci nejsou oprávněni:
   a) obcházet bezpečnostní mechanizmy prostředků výpočetní techniky;
   b) sdělovat své přístupové údaje k systémům ČNB;
   c) sdílet přístup k systémům ČNB (umožnit jinému pracovat pod uživatelovým oprávněním);
   d) provádět akce požadované třetí osobou (instalace softwaru, návštěva webových stránek apod.) bez ověření oprávněnosti požadavku.
7) Poskytovatel a jeho pracovníci jsou povinni:
   a) okamžitě nahlásit sekci informatiky ČNB, pokud identifikují možnost obejití bezpečnostních mechanizmů prostředků výpočetní techniky. To neplatí pro poskytovatele, jejichž předmět smlouvy/objednávky obsahuje tuto činnost;
   b) při opuštění pracovní stanice stanici uzamknout (např. vytažením multifukčního průkazu ze stanice) nebo se odhlásit a ověřit, že k odhlášení/uzamčení opravdu došlo;
   c) bezpečně zlikvidovat nepotřebná výměnná média (např. CD/DVD, flash disk, paměťová karta) prostřednictvím služby HelpDesku ČNB;
   d) bez prodlení odebrat z tiskárny vytištěné dokumenty, popřípadě pro zajištění důvěrnosti použít zabezpečený tisk, pokud to nastavení tiskárny umožňuje;
   e) v případě detekce viru nebo podezření na přítomnost škodlivého kódu neprodleně kontaktovat HelpDesk ČNB a stanici kompletně prověřit antivirovým programem za případné spolupráce HelpDesku ČNB.
8) Pracovníci poskytovatele nesmí:

a) zaznamenávat heslo tak, aby mohlo být snadno identifikováno (týká se i zapisování do elektronických dokumentů, např. Notepad). Pro uchování je možné použít například bezpečné úložiště na čipové kartě uživatele (SmartNotes);

b) používat stejná hesla v systémech ČNB a pro přístup do dalších systémů a aplikací mimo ČNB (např. soukromá e-mailová schránka, Facebook, LinkedIn).

9) Pracovníci poskytovatele nejsou oprávněni:

a) používat soukromou e-mailovou schránku pro činnosti související s plněním dle smlouvy/objednávky, kromě výjimečné situace, která nesnese odkladu a při níž hrozí nebezpečí z prodlení v případě nedostupnosti nebo poruchy pracovního e-mailu;

b) nastavovat automatické přeposílání e-mailů z pracovní e-mailové adresy mimo systémové prostředí ČNB;

c) ukládat jiné než veřejné informace mimo úložiště pod správou ČNB nebo poskytovatele (případně pod správou smluvně zajištěného partnera), zejména do cloudových služeb (např. uloz.to, leteckaposta.cz, Google Disk, Microsoft OneDrive a další).

10) Poskytovatel a jeho pracovníci nejsou oprávněni:

a) nepovoleně používat, kopírovat a šířit software, jako např.:

i) instalovat nebo spouštět na počítačích ČNB soukromě pořízený software (včetně softwaru licencovaného na uživatele jako soukromou osobu);

ii) instalovat nebo spouštět na počítačích ČNB z internetu stažený software (včetně komerčního software, software typu shareware, freeware, public domain a software licencovaného modelem GPL – General Public Licence). To neplatí v případech, kdy předmět smlouvy/objednávky obsahuje tuto činnost;

iii) instalovat či přenášet software ve vlastnictví ČNB na jiné počítače ČNB, na své soukromé počítače nebo na počítače třetích stran nebo pořizovat kopie softwaru instalovaného v počítači ČNB. To neplatí

(1) pro situace výslovně schválené a popsané v jiném vnitřním předpisu ČNB (např. vzdálený přístup ze zařízení, které není ve vlastnictví ČNB) a

(2) v případech, kdy předmět smlouvy/objednávky obsahuje tuto činnost;

b) používat nebo poskytnout neoprávněně jiným uživatelům sériová čísla, licenční klíče, hardwarové klíče nebo jiné technické prostředky sloužící k zajištění ochrany nebo jednoznačné identifikaci vlastníka licence softwaru získané v ČNB;

c) bránit spouštění nástrojů sloužících pro automatizované kontroly nainstalovaného a spouštěného softwaru a provádět činnosti, které by vedly ke zkreslení získaných dat z těchto nástrojů.

Archivace elektronické pošty

1) Zpráva zaslaná tak, že alespoň jedním z adresátů zprávy je emailová adresa ...@cnb.cz, se ukládá současně s přijetím i do dlouhodobého archivního úložiště.

2) Veškeré zprávy odesílané z emailové adresy ...@cnb.cz se ukládají do dlouhodobého archivního úložiště současně s odesláním.

Kontrola přístupu na Internet

Z důvodu zvláštní povahy činnosti ČNB a z toho plynoucí povinnosti zajištění bezpečnosti informačních systémů ČNB, z nichž některé jsou součástí kritické informační infrastruktury státu, jsou přístupy uživatelů na Internet ze sítě ČNB automaticky zaznamenávány na úrovni domén 2. řádu (tj. např. idnes.cz).

Příloha č. 8

Šablona realizační studie

[Pozn.: V níže uvedené šabloně lze přiměřeně měnit grafickou podobu a styl studie (fonty, formátování apod.), dále pak lze měnit/doplňovat/přizpůsobit členění kapitol v závislosti na nabízeném řešení služby a čitelnosti a srozumitelnosti textu. Nicméně struktura hlavních kapitol představuje rozsah oblastí, které by studie měla pokrýt a jejich zužování není povolena. V rámci podkapitol lze již úpravy připustit. ***Text kurzívou v hranatých závorkách je návodem, neměl by zůstat součástí výsledného dokumentu.****]*

ČESKÁ ČNB NÁRODNÍ BANKA

Projekt *ID projektu*

„*Název projektu*“

Realizační studie

Verze	
Datum verze	
Autor	
Vedoucí projektu *poskytovatele*	
Vedoucí projektu *objednatele*	

Historie změn

Verze	Datum	Autor	Popis změny

Obsah

1 Úvod

1.1 Účel dokumentu

[Dokument realizační studie popisuje způsob realizace, aktivace a následného provozu služby včetně analýzy funkčních požadavků, softwarové architektury a systémových požadavků tak, aby byla prokázána realizovatelnost všech objednatelem zadaných požadavků. ***Text kurzívou v hranatých závorkách je návodem, neměl by zůstat součástí výsledného dokumentu.****]*

1.2 Seznam pojmů a zkratek

[Výčet klíčových zkratek a pojmů s jejich vysvětlením]

Termín/Zkratka	Popis/Význam

Termín/Zkratka	Popis/Význam

1.3 Přehled použitých symbolů

[Popis použitých grafických symbolů v dokumentu]

Grafický symbol	Význam

2 Realizace věcného zadání

2.1 Analýza funkčních požadavků

[Kapitola obsahuje mapování funkčních požadavků na cílové řešení služby. Popis tak ve stručné formě představuje způsob realizace jednotlivých funkčních požadavků.]

2.2 Analýza bezpečnostních požadavků

[Kapitola obsahuje mapování funkčních požadavků na cílové řešení služby. Popis tak ve stručné formě představuje způsob realizace jednotlivých funkčních požadavků.]

2.3 Komunikační matice pro hlášení KBU/KBI

[Kapitola obsahuje popis komunikace mezi objednatelem a poskytovatelem]

Typ události	Popis	Formát komunikace	Odesílatel(é)	Příjemci
Kritický KBI	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 bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.	Telefonicky a e-mailem Detail analýzy do sdílené složky v Citrix ShareFile	Poskytovatel	Objednatel
Střední KBI	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 incidentu včetně minimalizace vzniklých škod.	Emailem a SMS Detail analýzy do sdílené složky v Citrix ShareFile	Poskytovatel	Objednatel
Nízký KBI	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 bezpečnostního incidentu včetně minimalizace vzniklých škod.	Emailem Detail analýzy do sdílené složky v Citrix ShareFile	Poskytovatel	Objednatel
KBU		Emailem Detail analýzy do sdílené složky v Citrix ShareFile	Poskytovatel	Objednatel

Požadavek na operativní analýzu KBU	dle odst. 2d), přílohy 2	Emailem	Objednatel	Poskytovatel
Požadavek na analytickou pomoc v případě potvrzeného KBI	dle odst. 2e), přílohy 2	Emailem a telefonicky	Objednatel	Poskytovatel
Návrhy vylepšení bezpečnostního monitoringu	dle odst. 2f), přílohy 2	Sdílená složka v Citrix ShareFile	Poskytovatel	Objednatel
Požadavek na doplnění analýzy, závazné pro řešení obdobných typů KBU/KBI	dle odst. 2 j) a k), přílohy 2	Emailem	Objednatel	Poskytovatel
Poučení o bezpečnosti IT	Požadavek na provedení poučení o bezpečnosti IT pracovníků SOC dle zaslaného vzoru.	Emailem	Objednatel	Poskytovatel
Zasílání měsíčního reportu	dle odst. 3a), přílohy 2	Sdílená složka v Citrix ShareFile	Poskytovatel	Objednatel
Ohlašování problémů s připojením VPN		Emailem	Poskytovatel	Objednatel
Ohlašování problémů s připojením SIEM/FlowMon		Emailem	Poskytovatel	Objednatel
Ohlašování plánovaných výpadků/změn SIEM, FlowMon a VPN		Emailem	Objednatel	Poskytovatel
Ostatní	Obecné informace	Emailem	Objednatel	Poskytovatel
Ostatní	Obecné informace	Emailem	Poskytovatel	Objednatel

Pověřené osoby smluvních stran a jejich kontaktní údaje, popř. bližší určení rozsahu pověření

Objednatel:

Poskytovatel:

[Uvedou se osoby, které s akceptací první etapy nahradí osoby podle čl. III odst. 3 smlouvy, a v případě potřeby se určí rozsah pověření jednotlivých pověřených osob nebo jejich skupin formou odkazů na konkrétní ustanovení smlouvy (vč. příloh)]

2.4 Pravidelný měsíční report

[Kapitola obsahuje definování struktury a obsahu měsíčního reportu]

3 Technická realizace řešení

3.1 Integrace s IS ČNB

3.1.1 SIEM objednatele

[Kapitola obsahuje návrh na úpravu obsahu v SIEM (pravidla, reporty apod.), které bude poskytovatel potřebovat pro zajištění kvality služby. Poskytovatel zajistí požadované úpravy v podobě balíčků pro nástroj ArcSight (v ČNB používaný SIEM) nebo přímo v systému SIEM objednatele v součinnosti s objednatelem. Všechny takové změny budou prováděny v sídle objednatele v běžnou pracovní dobu

objednatele (Po-Pá 7:45-16:15) a veškeré změny budou detailně zdokumentovány.
Kapitola může obsahovat i doporučení na sběr logů z dalších informačních systémů ČNB.]

3.1.2 Výpočetní prostředí ČNB
[Kapitola obsahuje závěr seznámení poskytovatele s kritičností jednotlivých IS objednatele, definování způsobu oznamování změn.]

3.1.3 VPN
[Kapitola obsahuje popis připojení poskytovatele k systému objednatele, definuje procesy při nástupu/ odchodu zaměstnance SOC, zneplatnění/obnovu certifikátu]

3.1.4 FlowMon objednatele
[Kapitola obsahuje návrh na úpravu obsahu v FlowMon, který bude poskytovatel potřebovat pro zajištění kvality služby.]

3.1.5 Další
[Kapitola obsahuje popis dalších (pokud existují) výše nepopsané interakce se službami systémového prostředí ČNB (např. e-mail).]

3.2 Bezpečnost a ochrana osobních údajů
[Kapitola obsahuje popis řešení z hlediska bezpečnosti, integrity a důvěrnosti dat.]

3.2.1 Autentizace a autorizace, řízení přístupu
[V podkapitole je popsán princip řízení přístupů k informacím resp. informačním aktivům: jakým prostřednictvím přistupují interní a externí uživatelé, způsob automatického blokování účtů uživatelů při ukončení zaměstnaneckého poměru, povolené protokoly apod.]

3.2.2 Logování
[V podkapitole je popsán způsob logování a monitorování logů, napojení na SIEM.]

3.2.3 Zabezpečení síťové komunikace a uložených dat
[V podkapitole je popsán způsob, jak je zabezpečena síťová komunikace a zabezpečení uložených dat.]

3.2.4 Plnění požadavků na ochranu osobních údajů

4 Návrh projektové realizace

4.1 Detailní harmonogram realizace
[Harmonogram realizace uvádí rozpad realizace projektu do jednotlivých etap a činností s ohledem na dodržení stanovených termínů/lhůt. Harmonogram musí obsahovat milníky pro předání díla nebo jeho částí k akceptačnímu řízení.]

5 Registr změn
[V kapitole je uveden seznam změn oproti předběžné studii/zadávací dokumentaci, jejich akceptace a jejich dopady do projektu – časové, zdrojové a finanční.]

ID změny	**Popis změny**	**Akceptována Ano/Ne**	**Realizace** (termín, zdroje a finance)