Prováděcí smlouva
číslo: S075/2018-C18

k Rámcové dohodě na poskytování služeb ze dne 7. 5. 2018

(dále též jen „**Prováděcí smlouva**“)

Smluvní strany:

Ústav zdravotnických informací a statistiky České republiky

Organizační složka státu

se sídlem: Palackého náměstí 4, PSČ 128 01 Praha 2

IČO: 00023833

bankovní spojení: [redacted]

zastoupen: prof. RNDr. Ladislavem Duškem, Ph.D. ředitelem

(dále jen „**Objednatel**“)

a

SKYLAB spol. s r.o.

se sídlem/místem podnikání: Zakouřilova 16/1170, 149 00 Praha 4

IČO: 25790943, DIČ: CZ25790943

subjekt zapsaný v obchodním rejstříku vedeném Městským soudem v Praze

spisová značka oddíl C, vložka 70554

bank. spojení: [redacted]

(dále jen „**Poskytovatel“)**

1. ÚVODNÍ USTANOVENÍ

1.1 Tato Prováděcí smlouva se uzavírá jako Prováděcí smlouva k Rámcové dohodě na poskytování služeb uzavřené mezi Objednatelem a Poskytovatelem dne 7. 5. 2018 (dále též jen „Rámcová dohoda“)

1.2 Veškeré pojmy uvedené v této Prováděcí smlouvě budou vykládány v souladu s jejich významem uvedeným v Rámcové dohodě.

1.3 Tato Prováděcí smlouva je uzavřena v souladu s postupem uvedeným v čl. 5 Rámcové dohody v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále též jen „ZZVZ“) na základě výzvy Objednatele k poskytnutí Podpůrných služeb specifikovaných v Příloze č. 1 této Prováděcí smlouvy (dále též jen „služby“).

2. PŘEDMĚT PLNĚNÍ

2.1 Poskytovatel se zavazuje poskytnout Objednateli služby v rozsahu uvedeném v Příloze č. 2 této Prováděcí smlouvy.

2.2 Součástí předmětu plnění bude vždy i zdokumentování provedených změn a také finálního stavu infrastruktury a konfigurací, které budou prováděny v rámci činností uvedených v příloze 1. Dokumentace bude předložena v rámci akceptační procedury.

2.3 Služby budou poskytnuty po dobu uvedenou v Příloze č. 3 této Prováděcí smlouvy.

2.4 Objednatel uhradí Poskytovateli za poskytnuté služby cenu za podmínek stanovených Rámcovou dohodou a Přílohou č. 1 této Prováděcí smlouvy.

2.5 Celková cena uvedená v Příloze č. 2 Prováděcí smlouvy, je cenou maximální a nepřekročitelnou a bude fakturována dle skutečně vykázaných nákladů.

3. ZÁVĚREČNÁ USTANOVENÍ

3.1 Práva a povinnosti Objednatele a Poskytovatele související s poskytování služeb dle této Prováděcí smlouvy se řídí Rámcovou dohodou, není-li v této Prováděcí smlouvě výslovně stanoveno jinak.

3.2 Tato Prováděcí smlouva je vyhotovena ve dvou stejnopisech, z nichž každá strana obdrží po jednom; Je-li podepsána elektronicky, pak je podepsána v jednom (1) originále pomocí uznávaných elektronických podpisů osob oprávněných jednat za smluvní strany.

3.3 Jakékoliv změny či doplnění této Prováděcí smlouvy mohou být učiněny výhradně písemným dodatkem schváleným oběma smluvními stranami.

3.4 Vztahuje-li se důvod neplatnosti jen na některé ustanovení Prováděcí smlouvy, je neplatným pouze toto ustanovení, pokud z jeho povahy nebo obsahu anebo z okolností, za nichž bylo ujednáno, nevyplývá, že jej nelze oddělit od ostatního obsahu Prováděcí smlouvy.

3.5 Nedílnou součástí této Prováděcí smlouvy tvoří následující přílohy:

Příloha č. 1 – Vymezení poskytovaných služeb
Příloha č. 2 – Rozsah poskytovaných služeb
Příloha č. 3 – Harmonogram plnění

Objednatel

[redacted]

Ústav zdravotnických informací a statistiky České republiky
prof. RNDr. Ladislav Dušek, Ph.D, ředitel

Poskytovatel

[redacted]

Příloha č. 1

Vymezení poskytovaných služeb

Předmět plnění:

Objednatel požaduje poskytnutí expertních služeb v souvislosti s vybudováním a provozem bezpečnostní dohledového centra (dále jen SOC) pro infrastrukturu Objednatele. Jedná se o provoz datových center resortních informačních systémů, základní infrastruktury pro provoz zásadních informačních systémů resortu zdravotnictví jakou jsou plánované systémy elektronického zdravotnictví IDRR, Národní zdravotnické registry NZIS a další provozní informační systémy. Pro tato datová centra Objednatel požaduje zajištění provozu bezpečnostní dohledového centra (dále jen SOC)

SOC provádí detekci potenciálního kybernetického bezpečnostního incidentu. Pro potřeby detekce realizuje SOC sběr a analýzu dat (logů) z různých zdrojů v rámci vymezeného perimetru a externí data o potenciálních hrozbách, a to jak na úrovni konkrétních IP adres, tak i na úrovni analýzy postupů a technik potenciálních útočníků. Důležitým úkolem SOC je také získávat a zpracovávat informace o zranitelnostech využívaného softwaru a hardwaru.

Konkrétní úkoly SOC

- Monitorování pokusů o průnik v rámci střeženého perimetru a ochrana proti nim,
- přímý zásah k omezení dopadů incidentu u datových center a koordinační činnost v rámci organizace,
- realizace procesu zvládání a ponaučení se z bezpečnostních incidentů,
- realizace zajištění kontinuity činností organizace (později resortu) při krizových situacích,
- zajištění souladu činnosti organizace s právními předpisy, jenž se týkají ochrany informací,
  a s interními předpisy organizace (včetně návrhu jejich změn),
- zpracování logů o událostech ze zařízení a aplikací na síti,
- zpracování, korelace a vyhodnocení shromážděných logů a flows v reálném čase,
- vyhodnocení detekce hrozeb APT a “Zero-Day“ útoků, včetně behaviorální analýzy,
- mMonitorování chování v síti,
- identifikace a kategorizace zranitelností,
- Informace o nalezené zranitelnosti, popis hrozby při jejím potenciálním zneužití a případné návrhy řešení, jak mezeru odstranit,
- vyhodnocování nalezených zranitelností a jejich prioritizace,
- realizace změnových požadavků v rámci provozovaných monitorovacích systémů.

Hlavním zdrojem, který bude SOC ÚZIS využívat je nástroj **IBM Security QRadar SIEM** v konfiguraci:

- **IBM Security QRadar SIEM Log Manager** – zabezpečuje technický sběr logů, jejich přijetí, normalizaci k zajištění jednotného vyhledávání logů a jejich bezpečné uložení.
- **IBM Security QRadar SIEM** – čerpá data z Log Managmentu a přidává systému logiku. Modul detekuje bezpečnostní události na základě korelace z příchozích logů a následně je prioritizuje dle závažnosti a dopadu.
- **IBM Security QRadar Vulnerability Manager** – doplňuje informace o konkrétních verzích software a hardware v infrastruktuře, o konkrétních zranitelnostech daných verzí a tím poskytuje přesnější detekci hrozeb.

Dalším zdrojem, který je již využíván, je **LOGmanager**, který tvoří centrální úložiště provozních a bezpečnostních záznamů. LOGmanager provádí záznam a analýzu systémových událostí z produkčních zařízení.

Důležitou roli zastává mezi provozovanými nástroji nástroj **IBM Resilient Security Orchestration Automation and Response Platform** (dále jen IBM Resillient). Nástroj je nastaven a plně integrován s nástrojem QRadar SIEM, taky aby při vzniku událostí odpovídající definovaným incidentům, operátor nástroje QRadar SIEM odeslal podrobnosti o této události do nástroje Resilient, kde je vytvořen záznam o incidentu. Do vytvořeného záznamu o incidentu jsou automaticky přidány kroky nutné k vyřešení incidentu. Postup řešení jednotlivých incidentů je nadefinován v nástroji Resilient podle typu incidentů. Operátor nástroje Resilient postupuje dle zobrazených kroků a po jejich splnění je označuje za splněné až do vyřešení incidentu. Po vyřešení incidentu je incident označen za uzavřený a automaticky se uzavře i událost v nástroji QRadar SIEM.

Objednatel dále požaduje poskytnutí služeb a zajištění zvýšeného dohledu technického prostředí pro provoz vyjmenovaných infomačních systémů a spojené technické infrastruktury:

Infrastruktura očkování

- [redacted]
- [redacted]

Infrastruktura EREG/ISIN

[redacted]

Servery obsluhující interní systémy, registry. Níže uvedená data jsou obecnou ukázkou registrů, se kterými se operátor dohledu nejčastěji přichází do styku především ze strany aktualizací technických pracovníků ÚZIS.

CUD – centrální úložiště dat
NRZP – národní registr zdravotnických pracovníků
ISPV – informační systém o průměrném výdělku
ISLPZ – informační systém, jehož účelem je získání informací o okolnostech úmrtí.
RZPRO – národní registr zdravotních prostředků
NRLUD – národní registr léčby uživatelů drog

Důležité odkazy:

[redacted]

[redacted]

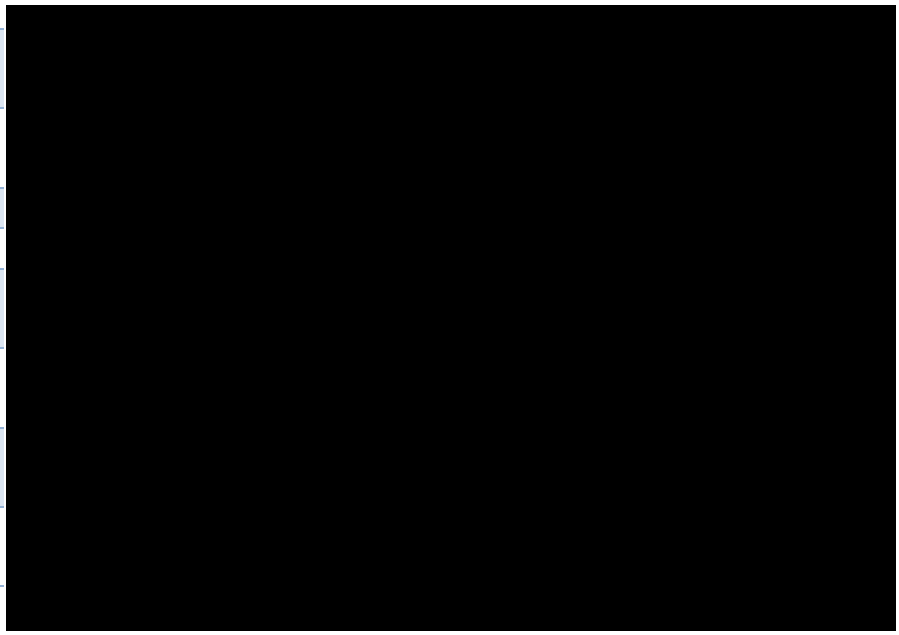
[redacted]

Webové služby

Webové služby budou monitorovány pomocí nástroje zajištěným dodavatelem dané služby a nástrojem Azure Insight.

Název služby	Externí adresa
ArcGis Proxy	[redacted]
CUD API pro čTečku a Tečku	
CUD API pro Policii	
CUD API pro Reservatic	
CUD API pro Tečku	
CUD API Vakcinace, lékové žádanky a další	
CUD Dávky - Form602 import	
CUD Dávky - Import - starý	
CUD Dávky - Import a stav dávek - aktuální	
CUD Dávky - Import alternativní	
CUD Dávky - Stav dávek - starý	
CUD Dávky - Zjištění verze	
CUD PLF (GUI)	
CUD Předběžný žádanka pro testy COVID-19 (GUI)	
CUD Ztotožnění z NIS	
CUD Ztotožnění z NIS - staré	

CUD Ztotožnění z NIS - staré WSDL	[redacted]
CUD Žádanky COVID-19 ověření	
CUD Žádanky COVID-19 ověření	
CUD Žádanky COVID-19 ověření - staré	
CUD Žádanky COVID-19 potvrzení	
CUD Žádanky COVID-19 potvrzení laboratoří	
CUD Žádanky COVID-19 založení	
CUD Žádanky COVID-19 založení	
CUV UlozitRozpracovanyVykaz Web Service	
HDM HZS Web Service	
HOK GRUP Web Service	
CHLAP Synchronizace offline verze	
ISIN Web CovItService	
ISIN Web IzsService	
ISIN Web MpsvService	
ISIN Web Service CfaClusterService	
ISIN Web Service DaktelaService	
ISLPZ CSUImportService Web Service	
JEHLA Web Service	
JTP IDT ClientSigningApp	
JTP Sms Dorucenky	
NOR Davka Web Service	
NRAR Web Service 1	
NROD Synchronizace Web Service	
NROD Synchronizace Web Service2	
NROVDK Web Service	

NRPZS Sluzba Web Service	
NRPZS Sluzba Web Service Export	
NRZP Web Service	
NRZP Web Service2	
RZPRO Sukl Web Service	
RZPRO Zadost Web Service	
TISSIS Sluzba Web Service	
TRINIS Sluzba Web Service	

Služba bude poskytována v třísměnném provozu jedním operátorem, přičemž třetí směna je pohotovostní. Na dohledovou službu bude navazovat expertní podpora v případě problému.

Požadavky na činnost provozního dohledu v režimu 06:00-23:00 x 7

Služby dohledu provozu aplikací budou prováděny v režimu 24x7 tzn., nonstop. Pracovník dohledu bude mít k dispozici nástroje provozního a bezpečnostního dohledu ÚZIS ČR Zabbix a SIEM, dále dohledovou webovou stránku aplikací.

Povinností pracovníků je:

- Od 6 do 23h - nepřetržité sledování parametrů
- Od 23 do 6h – pohotovostní služba a akční připravenost k zásahu

Sledované parametry:

- Provozních ukazatelů infrastruktury
  - Vytížení procesorů
  - Vytížení paměti
  - Vytížení a kapacita pevných disků
- Provozní situace aplikace CRS
  - Dostupnost aplikace
  - Dostupnost aplikačního serveru
  - Dostupnost databázového serveru
  - Aktuální počet spojení
- Situace kybernetické bezpečnosti
  - Sledování DDOS útoků
  - Sledování přetížení síťových prvků

- Sledování strojových útoků
- Sledování pokusů o zneužití aplikace
- Sledování pokusů o převzetí systému

Tuto činnost bude dohled vykonávat na všech prvcích infrastruktury dle výše uvedeného schématu. V rámci předání služby dohledu mezi jednotlivými směnami provede předávající směna přebírající zápis o proběhu směny na formuláři provozního deníku:

Protokol o průběhu dohledu				
Datum od		**Datum do**		
Čas od		**Čas do**		
Jméno a příjmení				
Událost	**Popis události**	**Protiopatření**	**Datum**	**Čas**

Typy událostí pro zaznamenání

- Technické incidenty dle eskalačních procedur
- Události kybernetické bezpečnosti dle eskalačních procedur
- Provozních ukazatelů infrastruktury
    - Vytížení procesorů nad 80%
    - Vytížení paměti nad 80%
    - Vytížení a kapacita pevných disků nad 70%
- Provozní situace aplikace CRS
    - Dostupnost aplikace – krátkodobé výpadky pod 1min
    - Dostupnost aplikačního serveru – krátkodobé výpadky pod 1min
    - Dostupnost databázového serveru – krátkodobé výpadky pod 20 vteřin
    - Aktuální počet spojení nad 100.000
- Situace kybernetické bezpečnosti
    - Sledování přetížení síťových prvků vytížení nad 80%
    - Sledování strojových útoků nad rámec běžných pokusů

- Sledování pokusů o zneužití aplikace počet pokusů o vyplnění úvodního formuláře nad 20x z jedné IP adresy během 3minut

Provozní deník bude zaslán po každé směně dohledu manažerovi kybernetické bezpečnosti [redacted] a dále bude předán následující směně jako podklad pro sledování a dodavatelem uložen pro závěrečnou zprávu.

V případě závažných událostí bude postupováno dle následujících eskalačních procedur:

Eskalační procedury			
Technické incidenty			
Typ	**Popis**	**Eskalační čas**	**Kontaktní list**
A	Aplikace nedostupná / nefunkční	5min od zjištění	[redacted]
B	Zpomalení aplikace	15 min od zjištění	
C	Výpadek infrastruktury	3min od zjištění	
D	Výpadek infrastruktury v jednom z datových center, druhé je provozu schopné	10min od zjištění	
Událost kybernetické bezpečnosti			
Typ	**Popis**	**Eskalační čas**	**Kontaktní list**
A	DDOS útok, hrozí zahlcení prostředí a výpadek služeb	3min od zjištění	[redacted]

B	Pokusy o zneužití systému, strojové útoky na aplikaci nebo infrastrukturu	5min od zjištění	[redacted]
C	Útoky síťové prvky, skenování portů, použití otevřených metod méně závažných útoků	2h od zjištění, v případě nezávažných útoků neohrožující provoz, předání v pracovní době formou emailového požadavku na protiopatření	

Příloha č. 2
Rozsah poskytovaných služeb

Podpůrné služby		Cena v Kč bez DPH za jeden člověkoden	Počet člověkodnů	Cena v Kč bez DPH
KL3.22	Expert pro oblast kybernetické bezpečnosti	[redacted]		
KL3.25	Operátor SIEM			
KL3.26	Expert pro vyhodnocování bezpečnostních incidentů (SIEM)			
KL3.27	Architekt ochrany TIF, specialista na budování SIEM systémů			
Celková cena v Kč bez DPH				**4 148 500 Kč**
Celková cena v Kč včetně DPH				**5 019 685 Kč**

Příloha č. 3

Harmonogram plnění

Předmět plnění	Termín plnění od	Termín plnění do
Poskytnutí expertních služeb v souvislosti s vybudováním a provozem bezpečnostní dohledového centra - SOC	1.1.2022	7.5.2022