MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Registr. číslo	PRÁVNÍ ODBOR **0131/ 21**

Prováděcí smlouva

k *Rámcové dohodě na poskytování služeb* ze dne 7. 5. 2018, ve smyslu *Dohody o přistoupení k rámcové dohodě a dodatku k rámcové dohodě* ze dne 2. 8. 2018

(dále jen „**Prováděcí smlouva**“)

Smluvní strany:

Česká republika – Ministerstvo zdravotnictví,

se sídlem: Palackého náměstí 4/375, Praha 2, PSČ 128 01

IČ: 00024341,

zastoupena: Ing. Martinem Zemanem, ředitelem odboru NCEZ

(dále jen „**Objednatel**“)

a

SKYLAB spol. s r.o.

se sídlem: 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

bankovní spojení: [redacted]., č. účtu: [redacted]

zastoupena: [redacted], jednatelem

(dále jen „**Poskytovatel“)**

Objednatel a Poskytovatel dále také jako „**smluvní strany**“ nebo jednotlivě jako „**smluvní strana**“

1. ÚVODNÍ USTANOVENÍ

1.1 Tato Prováděcí smlouva se uzavírá jako Prováděcí smlouva k *Rámcové dohodě na poskytování služeb* uzavřené dne 7. 5. 2018 mezi Poskytovatelem a Českou republikou – Ústavem zdravotnických informací a statistiky ČR (dále jen „Rámcová dohoda“), k níž Objednatel přistoupil jako třetí smluvní strana na základě *Dohody o přistoupení*

k rámcové dohodě a dodatku k rámcové dohodě ze dne 2. 8. 2018, registrované Objednatelem pod číslem 0608/18.

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, a na základě výzvy Objednatele k poskytnutí Podpůrných služeb specifikovaných v Příloze č. 1 této Prováděcí smlouvy (dále jen „služby“).

2. PŘEDMĚT PLNĚNÍ

2.1 Poskytovatel se zavazuje poskytnout Objednateli služby vymezené dle Přílohy č. 1 v rozsahu uvedeném v Příloze č. 2 této Prováděcí smlouvy.

2.2 Služby budou poskytovány do 365 dnů od podpisu smlouvy, nejdéle však do 30.04. 2022.

2.3 Poskytovatel se zavazuje služby poskytovat prostřednictvím osoby, která bude alespoň splňovat požadavky Objednatele na kvalifikaci dle Přílohy č. 3 této Prováděcí smlouvy.

2.4 Poskytovatel je povinen postupovat při plnění této Prováděcí smlouvy v souladu s interními předpisy Objednatele, které souvisí s kybernetickou bezpečností (zejména Politika bezpečnosti informací). Objednatel je povinen v případě změny interních předpisů o této změně informovat bez zbytečného odkladu Poskytovatele.

2.5 Pro účely akceptace poskytnutých služeb předloží Poskytovatel k poslednímu dni každého kalendářního měsíce Objednateli návrh akceptačního protokolu, jehož součástí bude přehled poskytnutých služeb a provedených činností (výkaz práce), společně s časovým údajem, které provádění činností skutečně trvalo.

2.6 Objednatel uhradí Poskytovateli za poskytnuté služby na základě jimi podepsaného akceptačního protokolu dle odstavce 2.5 tohoto článku cenu za podmínek stanovených Rámcovou dohodou a Přílohou č. 2 této Prováděcí smlouvy.

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

2.8 Poskytovatel je oprávněn při plnění této smlouvy komunikovat s příslušnými orgány ve věcech kybernetické bezpečnosti. Poskytovatel je povinen seznámit s obsahem sdělení Objednatele

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 třech stejnopisech, z nichž jeden stejnopis obdrží Poskytovatel a dva stejnopisy obdrží Objednatel.

3.3 Jakékoliv změny či doplnění této Prováděcí smlouvy mohou být učiněny výhradně písemným dodatkem podepsaným zástupcem každé ze smluvních stran. Jiná forma změny této Prováděcí smlouvy je vyloučena.

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 Tato Prováděcí smlouva je platná dnem jejího podpisu oběma smluvními stranami a účinná dnem jejího zveřejnění v registru smluv.

3.6 Nedílnou součástí této Prováděcí smlouvy jsou následující přílohy:

Příloha č. 1 – Vymezení poskytovaných služeb

Příloha č. 2 – Rozsah poskytovaných služeb

Příloha č. 3 – Požadavky na minimální kvalifikaci

Objednatel:

Česká republika – Ministerstvo zdravotnictví

V Praze dne _____

Ing. Martin Zeman

Digitálně podepsal Ing. Martin Zeman
Datum: 2021.03.02 09:24:43 +01'00'

.....

Ing. Martin Zeman

ředitel odboru IT a elektronizace zdravotnictví

Poskytovatel:

SKYLAB spol. s r.o.

V Praze dne _____

[redacted]

.....

[redacted], jednatel

Příloha č. 1

Vymezení poskytovaných služeb

Předmětem plnění dle této Prováděcí smlouvy je zajištění služeb dle katalogového listu č. KL 3.22 Expert pro oblast kybernetické bezpečnosti ve smyslu Rámcové dohody na poskytování služeb uzavřené mezi Objednatelem a Poskytovatelem dne 7. 5. 2018 v celkovém rozsahu nejvýše 180 člověkodní, prostřednictvím kterého bude Poskytovatel poskytovat Objednateli služby Manažera kybernetické bezpečnosti, přičemž těžiště poskytovaných služeb bude spočívat v následujících činnostech:

- prosazování bezpečnosti informací,
- spolupráce na vedení bezpečnostního týmu a koordinaci jeho činností,
- podpora řízení systému bezpečnosti informací a prosazování Bezpečnostní politiky informací,
- zajišťování aktualizace Bezpečnostní politiky informací,
- zajišťování tvorby a aktualizace Strategie kybernetické bezpečnosti,
- koordinace tvorby bezpečnostního konceptu organizace, konceptu plánu obnovy a ostatních dílčích konceptů a systémových bezpečnostních pravidel, jakož i vydávání doplňujících pravidel a vodítek celkové kybernetické bezpečnosti,
- iniciace, sledování a vyhodnocování implementace opatření kybernetické bezpečnosti,
- informování Výboru pro řízení kybernetické bezpečnosti o bezpečnostních incidentech, zjištěných neshodách a nedostatečné efektivnosti bezpečnostních opatření,
- informování vedení organizace a vedení ICT o aktuálním stavu systému řízení informační bezpečnosti,
- koordinace projektů spojených s kybernetickou bezpečností,
- zvládání kybernetických bezpečností událostí,
- ověření a vyšetření bezpečnostních incidentů,
- koordinace opatření ke zvýšení bezpečnostního povědomí v organizaci a školení kybernetické bezpečnosti,
- provádění činností stanovených plánem zvládání rizik a dohled nad splněním všech plánovaných úkolů,
- příprava podkladů pro přezkoumání systému řízení bezpečnosti informací,
- dokumentace systému řízení kybernetické bezpečnosti,
- komunikace s příslušnými státními orgány ve věcech kybernetické bezpečnosti.

Manažer kybernetické bezpečnosti

Manažer kybernetické bezpečnosti zodpovídá za plánování, organizování a řízení realizace opatření, projektů a programů k řízení bezpečnosti informací tak, aby bylo dosaženo cílů stanovených zákonem o kybernetické bezpečnosti a jeho prováděcími předpisy, a to ve stanoveném termínu a v rámci stanoveného rozpočtu. Role Manažera kybernetické bezpečnosti působí jako "kontaktní" osoba pro veškeré aspekty a otázky kybernetické bezpečnosti, která rovněž prosazuje a koordinuje úlohu systému řízení informační bezpečnosti v organizaci.

Pravomoci a odpovědnosti role

Manažer kybernetické bezpečnosti je osoba odpovědná za systém řízení bezpečnosti informací od prevence přes průběžné testování až po eliminaci následků a vyhodnocení „úspěšných“ kybernetických incidentů. Odpovídá za tvorbu a aktualizaci Strategie kybernetické bezpečnosti resortu MZ ČR a aktualizaci Bezpečnostní politiky informací MZ ČR.

Jako takový je i výkonným protějškem NÚKIB pro případy řešení kritických kybernetických bezpečnostních událostí.

Manažer kybernetické bezpečnosti bude rovněž zapojen ve všech důležitých projektech s dopadem na zpracování, přenos a ukládání informací, zavádění nových nebo změny existujících systémů a procedur s dopadem do informační bezpečnosti ve fázi jejich přípravy a aplikace.

Manažer kybernetické bezpečnosti bude rovněž seznámen se všemi projekty s dopadem na zpracování, přenos a ukládání informací, zavádění nových nebo změny existujících systémů a procedur s dopadem na bezpečnost informací. Cílem tohoto opatření je zajistit, že budou náležitě vzaty do úvahy veškeré aspekty kybernetické bezpečnosti ve fázích přípravy, realizace a implementace všech relevantních projektů.

Klíčové činnosti:

a) Odpovědnost za řízení systému řízení bezpečnosti informací.

b) Pravidelný reporting pro vrcholové vedení Objednatele.

c) Pravidelná komunikace s vrcholovým vedením Objednatele.

d) Předkládání Zpráv o hodnocení aktiv a rizik, Plánu zvládání rizik a Prohlášení o aplikovatelnosti výboru pro řízení kybernetické bezpečnosti.

e) Poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti ICT.

f) Komunikace s GovCERT/CSIRT.

g) Podílení se na procesu řízení rizik.

h) Koordinace řízení incidentů.

i) Vyhodnocování vhodnosti a účinnosti bezpečnostních opatření.

Příloha č. 2

Rozsah poskytovaných služeb

Podpůrné služby		**Počet člověkodnů**	**Cena v Kč bez DPH za jeden člověkoden**	**Cena v Kč vč. DPH**
KL3.22	Expert pro oblast kybernetické bezpečnostní	maximálně 180	9 000,- Kč	10 890,- Kč
Celková maximální cena v Kč bez DPH				1 620 000,- Kč
Celková maximální cena v Kč včetně DPH				1 960 200,- Kč

Příloha č. 3

Minimální požadavky na kvalifikaci

I) Vzdělání a praxe:

a) alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo

b) absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti.

II) Certifikace – alespoň jednu certifikaci z níže uvedených

a) Certified Information Security Manager (CISM),

b) Certified in Risk and Information Systems Control (CRISC),

c) Certified Information Systems Security Professional (CISSP), nebo

d) Manažer BI (akreditační schéma ČIA).