



OBJEDNÁVKA č. 0604/2022/EPCH/O

Odběratel

IČ: 70890692 DIČ: CZ70890692

Moravskoslezský kraj

28. října 2771/117

70218 Ostrava

Vyřizuje:

Telefon:

Odbor:

KŘ-4

Dodavatel

IČ: 28305043 DIČ: CZ28305043

MT Legal s.r.o., advokátní kancelář

Jana Babáka 2733/11

61200 Brno

Vyřizuje:

Telefon:

Objednáváme u Vás:

Předmětem této písemné výzvy je komplexní zajištění realizace zadávacího řízení **na řešení kybernetické bezpečnosti v nemocnicích MSK** pro Moravskoslezské datové centrum, příspěvkovou organizaci (to znamená pro tzv. **Dotčený subjekt**) v souladu s Rámcovou dohodou na zajištění komplexních služeb souvisejících s administrací zadávacích řízení včetně poskytování právního poradenství v oblasti veřejného investování č. 03339/2021/KŘ uzavřenou dne 16.07.2021.

Datum požadovaného splnění: do ukončení zadávacího řízení

Přílohy: písemná výzva k uzavření Prováděcí smlouvy

UPOZORNĚNÍ: Úhrada faktury se provádí 30. kalendářní den od data doručení faktury.

Povinnost zaplatit cenu je splněna dnem odepsání příslušné částky z účtu objednatele.

Odběratel uplatní institut zvláštního způsobu zajištění daně dle § 109a zákona o DPH a hodnotu plnění odpovídající dani z přidané hodnoty uvedené na faktuře uhradí v termínu splatnosti této faktury stanoveném dle objednávky přímo na osobní depozitní účet dodavatele vedený u místně příslušného správce daně v případě, že:

a) dodavatel bude ke dni uskutečnění zdanitelného plnění zveřejněn v aplikaci „Registr plátců DPH“ jako nespolehlivý plátcce, nebo

b) dodavatel bude ke dni uskutečnění zdanitelného plnění v insolvenčním řízení.

Odběratel nenese odpovědnost za případné penále a jiné postihy vyměřené či stanovené správcem daně dodavatel v souvislosti s potenciálně pozdní úhradou DPH, tj. po datu splatnosti této daně.

Dodavatel prohlašuje, že není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (člen vlády nebo vedoucí jiného ústředního správního úřadu, v jehož čele není člen vlády), nebo jím ovládaná osoba vlastní podíl představující alespoň 25% účast společníka v obchodní společnosti. Dodavatel bere na vědomí, že pokud je uvedené prohlášení nepravdivé, bude smlouva považována za neplatnou.

MAX. CENA CELKEM (vč. DPH)**114 950,00 Kč****Upřednostňujeme zaslání faktur elektronicky.**

e-mail pro zaslání faktury: posta@msk.cz

Název datové schránky: moravskoslezsky kraj

Identifikátor datové schránky: 8x6bxsd

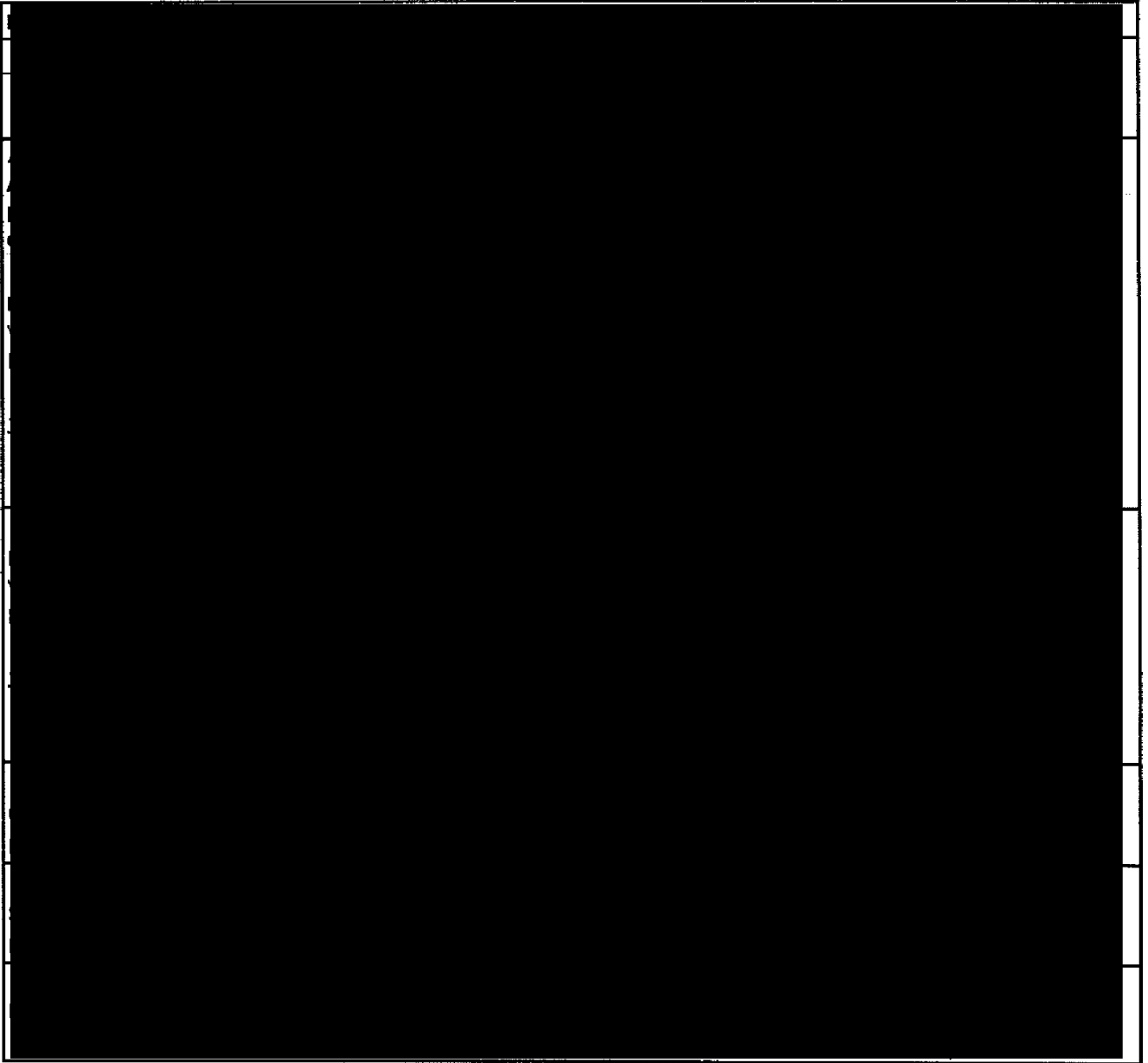
Číslo výdajového účtu : 27-1650676349/0800

Datum: 13.05.2022

MORAVSKOSLEZSKÝ KRAJ

Krajský úřad
28. října 117
702 18 OSTRAVA

-49-



Příloha k objednávce č. 0604/2022/EPCH/O

Písemná výzva k uzavření Prováděcí smlouvy

Identifikace zadávající organizace (Dotčený subjekt)	Moravskoslezské datové centrum, příspěvková organizace Na Jízdárně 2824/2, 702 00 Ostrava IČO: 06839517 [REDAKCE]
Kontaktní osoba	[REDAKCE]

Předmětem této písemné výzvy je komplexní zajištění realizace zadávacího řízení na řešení kybernetické bezpečnosti v nemocnicích MSK pro Moravskoslezské datové centrum, příspěvkovou organizaci v souladu s Rámcovou dohodou na zajištění komplexních služeb souvisejících s administrací zadávacích řízení včetně poskytování právního poradenství v oblasti veřejného investování č. 03339/2021/KŘ uzavřenou dne 16.07.2021.

1) **Název veřejné zakázky:** Řešení kybernetické bezpečnosti v nemocnicích MSK

2) **Druh zadávacího řízení:** otevřené řízení

3) **Předmět veřejné zakázky:**

Předmětem veřejné zakázky je implementace systému řízení bezpečnosti informací ISMS (Information Security Management System) a komplexní zajištění služeb centra kybernetické bezpečnosti SOC (Security Operations Center) k zajištění dohledu operátory, provozu nástrojů pro sběr a vyhodnocování kybernetických bezpečnostních událostí v provozovaných systémech a v komunikačních sítích se zajištěním prevence a aktivní reakce na případné kybernetické incidenty.

4) **Společný slovník pro veřejné zakázky CPV (klasifikace předmětu veřejné zakázky):**

Hlavní předmět: 72590000-7 Odborné počítačové služby
Další předmět: 72222300-0 Služby informačních technologií
72250000-2 Systémové a podpůrné služby
48200000-0 Balíky programů pro výstavbu sítí, internet a intranet
51610000-1 Instalace a montáž počítačů a zařízení pro zpracování dat

5) **Předpokládaná hodnota veřejné zakázky:**

81 455 098 Kč bez DPH / 98 560 669 Kč vč. DPH

6) **Požadavek na zpracování dokumentace nezbytné pro zahájení zadávacího řízení:**

do 10 kalendářních dnů.

7) **Další relevantní informace vztahující se k veřejné zakázce:**

Zakázka se vztahuje k projektu nebo programu financovanému z EU:
NE
Požadavek na uveřejnění předběžného oznámení:
NE
Veřejná zakázka rozdělena na části:
NE – odůvodnění: jedná se o komplexní službu, všechny požadované činnosti jsou provázány.
Informace o osobách odlišných od zadavatele, podílejících se na vypracování zadávací dokumentace (viz. § 36 odst. 4 zákona):
Revize podkladů pro technickou specifikaci dle zadávací dokumentace: Deloitte Advisory s.r.o., sídlem Italská 2581/67, Vinohrady, 120 00 Praha 2, IČO 27582167

<p>Informace o předběžné tržní konzultaci:</p> <p>Z předběžné tržní konzultace vychází také stanovení předpokládané hodnoty veřejné zakázky. Tímto průzkumem trhu (přiměřeně tak zohledněn také § 16 odst. 6 ZZVZ) bylo současně odpovídáno na dotazy níže uvedených 6 dodavatelů, proto je označujeme jako osoby, se kterými se vedla předběžná tržní konzultace.</p> <p>Osoby, které se na PTK podílely:</p> <p>TOTAL SERVIS a.s., sídlem Praha 10, Počernická 3226/2g, PSČ 10000, IČO 27234151 Axians redtoo s.r.o., sídlem Na strži 2097/63, Krč, 140 00 Praha 4, IČO 24236594 VISITECH a.s., sídlem Košínova 655/59, Královo Pole, 612 00 Brno, IČO 25543415 SOITRON s.r.o., sídlem Pekařská 621/7, Jinonice, 155 00 Praha 5, IČO 27270599 Atos IT Solutions and Services s.r.o., sídlem Praha 4 - Nusle, Doudlebská 1699/5, 140 00, IČO 44851391 AUTOCONT a.s., sídlem Hornopolská 3322/34, Moravská Ostrava, 702 00 Ostrava, IČO 04308697</p> <p>blíže viz dokument Průběh předběžné tržní konzultace</p>
<p>Místo plnění:</p> <p>nemocnice MSK</p>
<p>Prohlídka místa plnění:</p> <p>S ohledem na charakter veřejné zakázky zadavatel předpokládá, že nebude organizovat prohlídku místa plnění; dodavatelé jsou oprávněni o provedení prohlídky požádat v rámci institutu žádosti dle § 98 odst. 3 ZZVZ.</p>
<p>Lhůta plnění:</p> <p>48 měsíců od nabytí účinnosti smlouvy</p> <p>a) Prováděcí (implementační) projekt – do 1 měsíce od nabytí účinnosti této smlouvy, a to včetně zpracování připomínek objednatele a akceptace</p> <p>b) Základní implementace ISMS včetně školení – do 3 měsíců od nabytí účinnosti této smlouvy v rozsahu nutném pro zahájení poskytování služeb SOC; následné poskytování služeb ISMS po dobu neurčitou</p> <p>c) Adaptační fáze SOC – do 3 měsíců od nabytí účinnosti této smlouvy, a to včetně zpracování připomínek objednatele a akceptace,</p> <p>d) Provozní fáze SOC – po dobu neurčitou od akceptace výstupů z adaptační fáze SOC.</p>
<p>Množství nebo rozsah zakázky:</p> <p>Komplexní zajištění aktivní kybernetické bezpečnosti jako výstupu poskytovaných služeb, vyhodnocování kybernetických bezpečnostních událostí, provozních událostí ve výpočetních systémech a v komunikačních sítích u vyjmenovaných subjektů.</p>
<p>Opce:</p> <p>Zadavatel si vyhrazuje ve smyslu ust. § 100 odst. 3 ZZVZ (ve spojení s ust. § 66 ZZVZ) právo požadovat do 3 let ode dne uzavření smlouvy na plnění veřejné zakázky poskytnutí nových služeb spojených s implementací koncepce Hospital cloud a dále případně služeb (či jejich části) vymezených v odst. 3.1 shora ve vztahu k organizaci Zdravotnická záchranná služba Moravskoslezského kraje, příspěvková organizace, přičemž předpokládaná hodnota takových služeb činí do 20 mil. Kč bez DPH.</p>
<p>Doplňující informace:</p> <p><u>Technická kvalifikace:</u></p> <p>Ze seznamu významných zakázek musí jednoznačně vyplývat, že dodavatel v uvedeném období (tj. v posledních 5 letech před zahájením zadávacího řízení) realizoval alespoň tyto významné zakázky:</p> <p>1. 2 významné zakázky, jejichž předmětem (každé z nich) bylo poskytování služeb dohledového centra nad bezpečnostními událostmi a incidenty v rámci IS objednatele (SOC) alespoň po dobu 1 roku (tj. 12 po sobě jdoucích měsíců) ve finančním objemu nejméně 500.000 Kč bez DPH / 1 rok/ 1 zakázka poskytování těchto služeb, přičemž předmětem alespoň jedné z těchto zakázek byl také dohled nad:</p> <ul style="list-style-type: none"> • provozem prvků kritické informační infrastruktury ve smyslu ust. § 2 písm. b) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, nebo

- provozem významného informačního systému spravovaného orgánem veřejné moci ve smyslu ust. § 2 písm. d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, nebo
- provozem informačního systému základní služby ve smyslu ust. § 2 písm. j) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů;

2. **další 2 zakázky**, jejichž předmětem (každé z nich) bylo zavedení systému řízení bezpečnosti informací dle ČSN EN ISO/IEC 27001, vč. certifikace anebo implementace řízení bezpečnosti informací dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů s auditovaným výstupem shody (bez nezbytné certifikace implementovaného řešení); každá z takových služeb musela obsahovat minimálně projekt zahrnující vstupní analýzu, analýzu rizik a návrhy nebo zpracování či úpravu bezpečnostní dokumentace. Zadavatel požaduje, aby u nejméně 1 referenční zakázky byla koncovým odběratelem služby povinná osoba dle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů;

3. **další 2 zakázky**, jejichž předmětem (každé z nich) bylo provedení auditu kybernetické bezpečnosti v rozsahu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů; zadavatel požaduje, aby nejméně 1 referenční zakázka byla realizována u zdravotnického zařízení.

Není-li stanoveno jinak, kvalifikaci rovněž splní dodavatel v případě, že se jedná o významné zakázky zahájené dříve než v posledních 5 letech před zahájením zadávacího řízení, pokud byly v takových posledních 5 letech dokončeny, nebo pokud probíhaly i po zahájení zadávacího řízení, nebo pokud stále probíhají, za předpokladu splnění výše uvedených parametrů ke dni konce lhůty pro prokázání kvalifikace (tj. řádné dokončení příslušné části významné zakázky, která naplňuje požadavky zadavatele na reference).

Zadavatel současně uvádí, že s ohledem na omezení možnosti využití poddodavatele podle odst. 7.7. zadávací dokumentace musí část kvalifikace spočívající v plnění dle odst. 6.4 písm. a) bod 1 zadávací dokumentace prokázat účastník zadávacího řízení.

Dodavatel předloží doklady o odborné kvalifikaci pro následující osoby:

1. Manažer centra kybernetické bezpečnosti

- vysokoškolské vzdělání magisterského stupně,
- je držitelem platné certifikace z oblasti managementu kybernetické bezpečnosti (certifikace akreditovaná dle ISO/IEC 17024 nebo ISO 27001 anebo relevantní certifikace ISACA, nebo obdobný ekvivalent),
- má alespoň 5 let praxe za posledních 7 let před zahájením zadávacího řízení v oblasti kybernetické bezpečnosti (tato praxe musí vyplynout z profesního životopisu, kdy v každém příslušném roce dokládané praxe musela osoba vykázat alespoň jednu zkušenost v požadované oblasti; jedna zkušenost může být započítána i v rámci dvou (i více) let, a to za předpokladu, že v příslušném roce bylo plnění poskytováno alespoň po dobu 3 měsíců),

2. 3 osoby – Analytik kybernetické bezpečnosti

- vysokoškolské vzdělání bakalářského stupně,
- je držitelem platné technické certifikace na dodávanou technologii v rámci nabízených služeb a certifikace CompTIA Sec+, CySa+ nebo obdobné,
- má alespoň 3 roky praxe za posledních 5 let před zahájením zadávacího řízení v oblasti kybernetické bezpečnosti,
- má alespoň 1 zkušenost za posledních 5 let před zahájením zadávacího řízení s poskytováním služeb dohledového centra nad bezpečnostními událostmi a incidenty (SOC) v rámci IS objednatel zahrnujícího sběr logů z více než 100 zařízení a vyhodnocováním logů s cílem identifikovat potenciální bezpečnostní incidenty,

S ohledem na omezení možnosti využití poddodavatele podle odst. 7.7. zadávací dokumentace nesmí být tato role zajišťována prostřednictvím poddodavatele.

3. 1 osoba – Forenzní analytik

- vysokoškolské vzdělání magisterského stupně,

- je držitelem platné technické certifikace související s technologií nabízených služeb v oblasti kybernetické bezpečnosti a certifikace CompTIA Sec+, CySa+, CEH nebo obdobné,
- má alespoň 5 let praxe za posledních 7 let před zahájením zadávacího řízení v oblasti kybernetické bezpečnosti (tato praxe musí vyplynout z profesního životopisu, kdy v každém příslušném roce dokládané praxe musela osoba vykázat alespoň jednu zkušenost v požadované oblasti; jedna zkušenost může být započítána i v rámci dvou (i více) let,
- má alespoň 1 zkušenost za posledních 5 let před zahájením zadávacího řízení se zpracováním informací o kybernetických bezpečnostních událostech a incidentech s využitím specializovaných metod analýzy dat a technik pro získávání důkazů souvisejících s případnou trestní činností,

S ohledem na omezení možnosti využití poddodavatele podle odst. 7.7. zadávací dokumentace nesmí být tato role zajišťována prostřednictvím poddodavatele.

4. 4 osoby – Operátor SOC

- středoškolské vzdělání ukončené maturitní zkouškou,
- je držitelem platné technické certifikace pro produkty s primární využitím v oblasti kybernetické bezpečnosti, a to alespoň základní úrovně,
- má alespoň 1 rok praxe za posledních 5 let před zahájením zadávacího řízení při poskytování ICT služeb v úrovni L1,
- má alespoň 1 zkušenost za posledních 5 let před zahájením zadávacího řízení se základní obsluhou provozovaných systémů v rámci SOC, a to nejméně po dobu 6 po sobě jdoucích měsíců,

S ohledem na omezení možnosti využití poddodavatele podle odst. 7.7. zadávací dokumentace nesmí být tato role zajišťována prostřednictvím poddodavatele.

5. 2 osoby – Bezpečnostní expert na síťové prvky včetně Firewall

- vysokoškolské vzdělání alespoň bakalářského stupně,
- je držitelem platné technické certifikace na technologii provozovanou ve zdravotnickém zařízení,
- má alespoň 5 let praxe za posledních 7 let před zahájením zadávacího řízení v oblasti kybernetické bezpečnosti (tato praxe musí vyplynout z profesního životopisu, kdy v každém příslušném roce dokládané praxe musela osoba vykázat alespoň jednu zkušenost v požadované oblasti; jedna zkušenost může být započítána i v rámci dvou (i více) let, a to za předpokladu, že v příslušném roce bylo plnění poskytováno alespoň po dobu 3 měsíců),
- má alespoň 1 zkušenost za posledních 5 let před zahájením zadávacího řízení se zpracováním bezprostředních incidentů v rámci řešení aktivních bezpečnostních opatření k zamezení kybernetického útoku ve specifických oblastech vztažených k síťovým prvkům včetně firewallů, spočívající v pokročilejší konfiguraci, monitoringu a technických konzultacích,
- byl v pozici bezpečnostního experta na síťové prvky včetně firewallů v posledních 5 letech před zahájením zadávacího řízení minimálně u 1 zakázky v oblasti kybernetické bezpečnosti,

S ohledem na omezení možnosti využití poddodavatele podle odst. 7.7. zadávací dokumentace nesmí být tato role zajišťována prostřednictvím poddodavatele.

6. 2 osoby – Bezpečnostní technologický expert pro oblast operačních systémů

- má alespoň 5 let praxe za posledních 7 let před zahájením zadávacího řízení v oblasti kybernetické bezpečnosti,
- má alespoň 1 zkušenost za posledních 5 let před zahájením zadávacího řízení se zpracováním bezprostředních incidentů v rámci řešení aktivních bezpečnostních opatření k zamezení kybernetického útoku ve specifických oblastech vztažených k operačním systémům Microsoft Windows a Linux, spočívající v pokročilejší konfiguraci, monitoringu, aktualizacích a technických konzultacích,
- je držitelem platného certifikátu v úrovni Microsoft Certified Associate (MCSA) nebo Microsoft Certified Solutions Expert (MCSE) nebo obdobného.

S ohledem na omezení možnosti využití poddodavatele podle odst. 7.7. zadávací dokumentace nesmí být tato role zajišťována prostřednictvím poddodavatele.

7. 2 osoby – Bezpečnostní technologický expert pro oblast databází

- má alespoň 5 let praxe za posledních 7 let před zahájením zadávacího řízení v oblasti kybernetické bezpečnosti,
- má alespoň 1 zkušenost za posledních 5 let před zahájením zadávacího řízení se zpracováním bezprostředních incidentů v rámci řešení aktivních bezpečnostních opatření k zamezení

kybernetického útoku ve specifických oblastech vztažených k databázím, spočívající v pokročilejších úpravách, aktualizacích, optimalizacích a technických konzultacích,

- je držitelem platného certifikátu v úrovni Microsoft Certified Associate (MCSA) nebo Microsoft Certified Solutions Expert (MCSE) nebo obdobného.

S ohledem na omezení možnosti využití poddodavatele podle odst. 7.7. zadávací dokumentace nesmí být tato role zajišťována prostřednictvím poddodavatele.

8. 2 osoby – Bezpečnostní technologický expert pro serverovou infrastrukturu včetně VMware

- má alespoň 5 let praxe za posledních 7 let před zahájením zadávacího řízení v oblasti kybernetické bezpečnosti,
- má alespoň 1 zkušenost za posledních 5 let před zahájením zadávacího řízení se zpracováním bezprostředních incidentů v rámci řešení aktivních bezpečnostních opatření k zamezení kybernetického útoku ve specifických oblastech vztažených k serverové infrastruktuře včetně VMware, spočívající v pokročilejší konfiguraci, monitoringu a technických konzultacích,
- je držitelem platného certifikátu VMware Certified Professional (VCP) nebo VMware Certified Advanced Professional (VCAP) nebo obdobného,

S ohledem na omezení možnosti využití poddodavatele podle odst. 7.7. zadávací dokumentace nesmí být tato role zajišťována prostřednictvím poddodavatele.

9. 2 osoby – Bezpečnostní technologický expert SIEM a Log Management

- je držitelem platné certifikace expertní úrovně na nabízené službě,
- má alespoň 2 roky praxe za posledních 5 let před zahájením zadávacího řízení v oblasti nástrojů SIEM a Log Managementu,
- byl v pozici technologického bezpečnostního experta v posledních 5 letech před zahájením zadávacího řízení minimálně u 2 zakázek v oblasti kybernetické bezpečnosti, přičemž tyto zakázky (každá z nich) zahrnovaly nastavení, analýzu událostí, návrh a ladění pravidel, napojení zdrojů logů, návrh a ladění parserů zdrojů logů,

S ohledem na omezení možnosti využití poddodavatele podle odst. 7.7. zadávací dokumentace nesmí být tato role zajišťována prostřednictvím poddodavatele.

10. 1 osoba – Bezpečnostní expert na hardening

- je držitelem platné expertní certifikace na Vulnerability Management System (VMS) technologii,
- má alespoň 5 let praxe za posledních 7 let před zahájením zadávacího řízení v oblasti kybernetické bezpečnosti (tato praxe musí vyplynout z profesního životopisu, kdy v každém příslušném roce dokládané praxe musela osoba vykázat alespoň jednu zkušenost v požadované oblasti; jedna zkušenost může být započítána i v rámci dvou (i více) let, a to za předpokladu, že v příslušném roce bylo plnění poskytováno alespoň po dobu 3 měsíců),
- má zkušenosti v posledních 5 letech před zahájením zadávacího řízení v oblasti kybernetické bezpečnosti ve funkci bezpečnostní specialista na VMS technologii (technologii skeneru zranitelnosti), a to minimálně u 5 projektů,

S ohledem na omezení možnosti využití poddodavatele podle odst. 7.7. zadávací dokumentace nesmí být tato role zajišťována prostřednictvím poddodavatele.

11. 4 osoby – Konzultant ISMS

- středoškolské vzdělání ukončené maturitní zkouškou,
- je držitelem platného certifikátu Lead auditor ISMS, případně manažer ISMS nebo manažer kybernetické bezpečnosti,
- má alespoň 3 roky praxe za posledních 5 let před zahájením zadávacího řízení na pozici konzultanta ISMS (tato praxe musí vyplynout z profesního životopisu, kdy v každém příslušném roce dokládané praxe musela osoba vykázat alespoň jednu zkušenost v požadované oblasti; jedna zkušenost může být započítána i v rámci dvou (i více) let, a to za předpokladu, že v příslušném roce bylo plnění poskytováno alespoň po dobu 3 měsíců),
- má alespoň 1 zkušenost v posledních 5 letech před zahájením zadávacího řízení v oblasti implementace Information Security Management System (ISMS) ISO/IEC 27001 nebo QMS ISO 9001,

12. 1 osoba – Auditor ISMS

- vysokoškolské vzdělání alespoň bakalářského stupně,
- je držitelem platné certifikace (dle ISO 27001) Certified Information System Auditor (CISA), Lead Auditor ISMS nebo ekvivalentu uvedené certifikace,
- má alespoň 3 roky praxe za posledních 5 let před zahájením zadávacího řízení na pozici auditora ISMS či auditora kybernetické bezpečnosti (tato praxe musí vyplynout z profesního životopisu, kdy v každém příslušném roce dokládané praxe musela osoba vykázat alespoň jednu zkušenost v požadované oblasti; jedna zkušenost může být započítána i v rámci dvou (i více) let,
- má alespoň 1 zkušenost v posledních 5 letech před zahájením zadávacího řízení v oblasti auditu nebo implementací Information Security Management System (ISMS) ISO/IEC 27001 nebo QMS ISO 9001,

13. 2 osoby – Školitel ISMS

- středoškolské vzdělání ukončené maturitní zkouškou,
- má alespoň 2 roky praxe za posledních 5 let před zahájením zadávacího řízení na pozici školitele ISMS (tato praxe musí vyplynout z profesního životopisu, kdy v každém příslušném roce dokládané praxe musela osoba vykázat alespoň jednu zkušenost v požadované oblasti; jedna zkušenost může být započítána i v rámci dvou (i více) let,

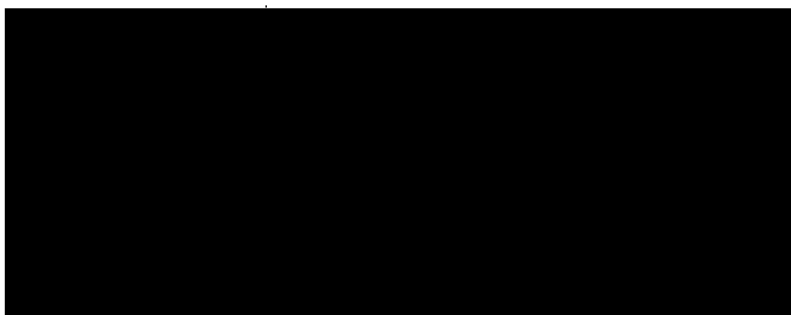
14. Projektový manažer pro implementaci ISMS

- vysokoškolské vzdělání magisterského stupně,
- je držitelem platného certifikátu projektového řízení PRINCE2 Practitioner, IPMA:C, PMI nebo obdobného,
- koordinoval v pozici projektového manažera (nebo v pozici s obdobnou odpovědností) za posledních 7 let před zahájením zadávacího řízení alespoň ve 2 případech tým při poskytování služeb v oblasti kybernetické bezpečnosti (např. služby dohledového centra anebo při implementaci řízení bezpečnosti informací).

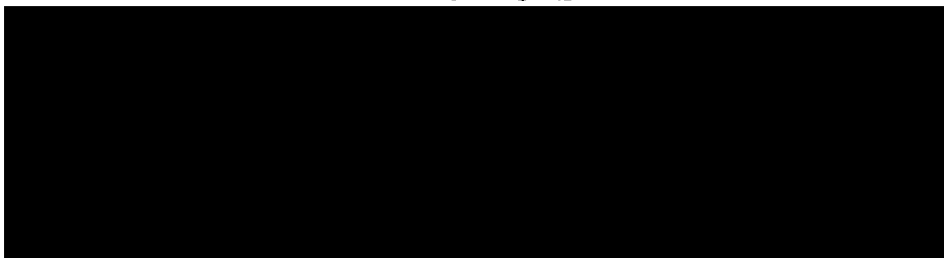
S níže uvedenými výjimkami zadavatel stanoví, že jedna osoba může zastávat více rolí, pokud budou doloženy shora uvedené požadavky zadavatele v plném rozsahu, avšak nikoliv více než 2 role za jednoho člena realizačního týmu. Zadavatel současně stanoví, že role analytika kybernetické bezpečnosti (tj. osoby shora uvedené pod č. 2) a operátorů SOC (tj. osoby shora uvedené pod č. 4) musí zastávat vždy samostatná (odlišná) osoba bez možnosti kumulaci rolí.

Zadavatel současně uvádí, že s ohledem na omezení možnosti využití poddodavatele podle odst. **Chyba! Nenalezen zdroj odkazů.** musí část kvalifikace spočívající v plnění dle bodů 2 až 10 prokázat účastník zadávacího řízení, tzn. nemůže se jednat o poddodavatele, ale osobu v pracovním poměru s účastníkem či osobu vykonávající práci na základě dohody o pracovní činnosti anebo dohody o provedení práce

8) Členové hodnotící komise za zřizovatele, tj. Moravskoslezský kraj



9) Návrh hodnotící komise za Dotčený subjekt



Předmět: RE: Objednávka – písemná výzva k uzavření Prováděcí smlouvy_VZ Řešení kybernetické bezpečnosti v nemocnicích MSK

From: [REDACTED]

Sent: Wednesday, May 18, 2022 11:32 AM

To: [REDACTED]

Cc: [REDACTED]

Subject: RE: Objednávka – písemná výzva k uzavření Prováděcí smlouvy_VZ Řešení kybernetické bezpečnosti v nemocnicích MSK

Dobrý den,

Potvrzuji přijetí písemné výzvy a přeji příjemný den

[REDACTED]



MT Legal s.r.o., advokátní kancelář

Praha | Brno | Ostrava

Jana Babáka 2733/11

612 00 Brno – Královo Pole

www.mt-legal.com

From: [REDACTED]

Sent: Friday, May 13, 2022 1:31 PM

To: [REDACTED]

Cc: [REDACTED]

Subject: Objednávka – písemná výzva k uzavření Prováděcí smlouvy_VZ Řešení kybernetické bezpečnosti v nemocnicích MSK

Vážení obchodní přátelé,

přílohou tohoto e-mailu Vám zasíláme písemnou výzvu k uzavření Prováděcí smlouvy v souladu s Rámcovou dohodou na zajištění komplexních služeb souvisejících s administrací zadávacích řízení včetně poskytování právního poradenství v oblasti veřejného investování č. 03339/2021/KŘ uzavřenou dne 16.07.2021, a to k realizaci veřejné zakázky pro Moravskoslezské datové centrum, příspěvkovou organizaci Moravskoslezského kraje (to znamená pro tzv. **Dotčený subjekt**) s označením » **Řešení kybernetické bezpečnosti v nemocnicích MSK** «.

Číslo objednávky: **0604/2022/EPCH/O**

V souladu s čl. VIII odst. 3 Rámcové dohody Vás žádáme o potvrzení této písemné výzvy na tuto e-mailovou adresu.

Děkuji a přeji Vám krásný víkend

[REDACTED]

odbor kancelář ředitele krajského úřadu

Předmět:

RE: Objednávka – písemná výzva k uzavření Prováděcí smlouvy_VZ Řešení kybernetické bezpečnosti v nemocnicích MSK

From: [REDACTED]

Sent: Wednesday, May 18, 2022 8:33 PM

To: [REDACTED]

Cc: [REDACTED]

Subject: RE: Objednávka – písemná výzva k uzavření Prováděcí smlouvy_VZ Řešení kybernetické bezpečnosti v nemocnicích MSK

Přeji pěkný den,

viz žádost níže uděluji souhlas s uzavřením Prováděcí smlouvy 0604/2022/EPCH/O.

Děkuji!



msdc

Se srdečným pozdravem

[REDACTED]

Moravskoslezské datové centrum, příspěvková organizace
Na Jízdárně 2824/2, 702 00 Ostrava

Mobil: [REDACTED]

E-mail: [REDACTED]

<https://www.msdc.cz/>



♻️ Zvažte, prosím, zda je nutno tuto zprávu vytisknout! Šetřeme naše životní prostředí!