KUJCP01BQZMP

Smlouva o zajištění funkce manažera kybernetické bezpečnosti

JON/01NF/024/21

dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník

Níže uvedeného dne, měsíce a roku se dohodly smluvní strany:

Jihočeský kraj
Sídlo: U Zimního stadionu 1952/2, 370 76 České Budějovice
Zastoupený: Ing. Petrem Vobejdou, vedoucím odboru informatiky
IČO: 70890650
DIČ: CZ70890650
Bankovní spojení: ČSOB, a.s.
Číslo účtu: 199783072/0300
Objednatel je plátcem DPH

(dále jen „Objednatel")

a

Ing. Martin Havel, MBA
Sídlo: Velešovická 20, 683 01 Rousínov
IČO:66565090
DIČ: CZ7101084364
Bankovní spojení: Česká spořitelna a.s.
Číslo účtu: 1153773033/0800
Poskytovatel je plátcem DPH

(dále jen „Poskytovatel")

na uzavření smlouvy o spolupráci (dále jen smlouva) níže uvedeného obsahu:

Čl. I. Předmět smlouvy

1.1 Poskytovatel se na základě této smlouvy zavazuje pro Objednatele vykonávat zejména tyto činnosti:

a) Seznámit se s veškerou interní dokumentací Objednatele, která má vztah k Systému řízení bezpečnosti informací dle požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a jeho prováděcích vyhlášek (dále jen „ZoKB"), případně má vztah na další související témata, viz např. problematika ochrany osobních údajů, GDPR, apod. a tuto dokumentaci pochopit včetně reálných dopadů do procesů, systému řízení bezpečnosti informací a fungování organizace Objednatele.
b) Zajistit vedení a průběžnou aktualizaci dokumentace Systému řízení bezpečnosti informací Objednatele dle požadavků ZoKB a prováděcích vyhlášek k ZoKB, případně dle požadavků legislativy ČR a EU související s oblastí kybernetické bezpečnosti, resp. systémem řízení bezpečnosti informací a dále na základě požadavků Objednatele. Poskytovatel je povinen z vlastní iniciativy navrhovat úpravy a aktualizace dokumentace Systému řízení bezpečnosti informací, spolupracovat na úpravách a aktualizacích navržených ze strany objednatele a zajistit promítnutí schválených změn, úprav a aktualizací do dokumentace Systému řízení bezpečnosti informací.
c) Zajišťovat plnění požadavků dle ZoKB, prováděcích vyhlášek k ZoKB a interní dokumentace Objednatele k Systému řízení bezpečnosti informací, zejména vykonávat funkci Manažera kybernetické bezpečnosti - tj. aktivně řešit a vést systém řízení bezpečnosti informací Objednatele.
d) Podílet se na aktualizaci Systému řízení bezpečnosti informací dle požadavků zákona ZoKB a jeho prováděcích vyhlášek.
e) Dle požadavků Objednatele aktivně řešit proces Řízení - Provozování - Monitorování a přezkoumání - Udržování a zlepšování ISMS v souladu s ZoKB.
f) Při výkonu svojí funkce se řídí pokyny vedoucího odboru informatiky.
g) Při výkonu svojí funkce bude úzce spolupracovat s interním zaměstnancem zařazeným na funkční místo „manažer kybernetické bezpečnosti", a dalšími určenými zaměstnanci odboru informatiky.
h) Poskytovatel bude vést, vytvářet a činit další úkony pro Objednatele v sídle Objednatele, v sídle Poskytovatele a formou dálkového přístupu.

1.2 Objednatel se zavazuje za poskytnuté plnění Poskytovatelem zaplatit Poskytovateli odměnu ve výši uvedené v článku III. této smlouvy.

1.3 Poskytovatel prohlašuje, že je na základě živnostenského oprávnění Poradenská a konzultační činnost a více jak 10 let praxe v oboru informační / kybernetické bezpečnosti oprávněn k výkonu této činnosti.

Čl. II. Termín plnění

2.1 Tato smlouva se uzavírá na dobu určitou a to na 3 roky od data účinnosti smlouvy (viz článek V. bod 5.1).

2.2 Kterákoliv ze smluvních stran je oprávněna vypovědět tuto smlouvu kdykoliv bez udání důvodu s výpovědní dobou 3 měsíců, která počíná běžet prvním dnem měsíce následujícího po doručení výpovědi druhé smluvní straně.

Čl. III. Cena

3.1 Za Předmět této smlouvy náleží Poskytovateli následující odměna:
Odměna je stanovena dle rozsahu provedených služeb ze strany Poskytovatele uvedeného v čl. I, bod 1.1 této smlouvy, a to ve výši **10.900,- Kč bez DPH**, **13 189,- Kč včetně DPH**, měsíčně.

3.2 Odměna bude hrazena vždy jedenkrát měsíčně za služby provedené v předchozím měsíci, a to na základě daňového dokladu (faktury) vystaveného/vystavené Poskytovatelem po skončení kalendářního měsíce. Daňový doklad/faktura může být zaslán/zaslána i elektronicky a musí korespondovat s předmětem této smlouvy, viz článek I. smlouvy. Splatnost daňového dokladu smluvní strany sjednaly na 14 dnů od data doručení daňového dokladu/faktury Objednateli. Dnem zaplacení je den odepsání příslušné částky z účtu Objednatele.

3.3 Náležitosti faktury
Faktury musí obsahovat všechny náležitosti daňového dokladu uvedené v § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Faktura musí dále obsahovat:

- označení dokladu (faktura)
- číslo smlouvy
- předmět plnění a jeho přesnou specifikaci ve slovním vyjádření (nestačí pouze odkaz na číslo uzavřené smlouvy)
- datum uskutečnění zdanitelného plnění, den odeslání a datum splatnosti
- označení banky a čísla účtu, na který budou poukázány finanční prostředky
- konečný příjemce a místo určení
- IČO smluvních stran

Čl. IV. Mlčenlivost

4.1 Smluvní strany se dohodly, že veškeré skutečnosti, které nejsou běžně dostupné v obchodních kruzích a se kterými přijdou do styku, tvoří předmět obchodního tajemství.

4.2 V souvislosti s předmětem plnění této smlouvy obdržel Poskytovatel, resp. obdrží od Objednatele důvěrné informace, ústní informace, jakož i znalosti a zkušenosti - následně zvané „Informace".

4.3 Poskytovatel se zavazuje, že:

a) nebude třetím osobám poskytovat žádné Informace získané od Objednatele,
b) informace a s nimi získané know-how bude používat pouze pro účely plnění povinností dle této smlouvy, nikoli pro vlastní potřebu, výrobu nebo pro dodávky konkurentům Objednatele,
c) informace zpřístupní pouze omezenému okruhu pracovníků Poskytovatele, kteří jsou určení k plnění povinností Poskytovatele dle této smlouvy,
d) učiní vhodná opatření a zajistí, aby pracovníci Poskytovatele udržovali v tajnosti informace Objednatele ve stejném rozsahu jako Poskytovatel a používali je pouze pro účely plnění povinností dle této smlouvy.

4.4 Všechny Objednatelem poskytnuté Informace a další podklady včetně výkresů, náčrtků a vzorků zůstávají výhradně vlastnictvím Objednatele. Informace a podklady nesmí být Poskytovatelem rozmnožovány/kopírovány.

4.5 Závazek mlčenlivosti končí po dvou letech od data ukončení této smlouvy.

Čl. V. Závěrečná ustanovení

5.1 Tato smlouva se uzavírá na dobu určitou, a to od 13. 11. 2021 na tři roky. Tato smlouva nabývá platnosti dnem podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem 13. 11. 2021. V případě, že k podpisu smlouvy nebo jejímu zveřejnění v registru smluv dojde až po 13. 11. 2021, nabývá smlouva účinnosti dnem zveřejnění v registru smluv.

5.2 Smlouva může být změněna pouze se souhlasem obou stran, formou písemných vzestupně číslovaných dodatků.

5.3 Právní vztahy neupravené touto smlouvou se řídí příslušnými ustanoveními Občanského zákoníku v platném znění.

5.4 Poskytovatel se zavazuje postupovat podle přílohy č. 1 této smlouvy – Bezpečnostní pravidla pro dodavatele.

5.5 Smlouva je uzavírána v elektronické podobě, kdy každá ze stran obdrž její elektronický originál opatřený elektronickými podpisy. Pokud smlouva není uzavírána v elektronické podobě, ale v podobě listinné, je vyhotovena ve 2 stejnopisech, kdy každá ze stran obdrží 1 vyhotovení.

5.6 Po přečtení této smlouvy účastníci prohlašují, že byla sepsána na základě jejich vážné a svobodné vůle, nebyla sepsána v tísni, jejímu obsahu rozumí a na důkaz svého souhlasu s jejím obsahem připojují své vlastnoruční podpisy.

Příloha č. 1 – Bezpečnostní pravidla pro dodavatele

V Českých Budějovicích dne 21-10-2021

V Rousínově dne 14.10.2021

Za Objednatele

Za Poskytovatele [redacted]

Bezpečnostní pravidla pro Dodavatele

Cílem těchto bezpečnostních pravidel je snižování kybernetických rizik a zvyšování účinnosti bezpečnostních opatření chránící Aktiva KÚ JK, ke kterým mají přístup Dodavatelé.

A.1 Základní odpovědnosti Dodavatele

Dodavatel řešení:

a. Je povinen dodržovat požadavky na bezpečnost informací v souladu s platnými zákony ČR.
b. Odpovídá za své řešení/dodávku/správu tak, aby respektovalo požadavky na bezpečnost KÚ JK, zabránilo bezpečnostním incidentům a stavu kybernetického nebezpečí.
c. Odpovídá za dodávku a implementaci řešení v požadované kvalitě i z pohledu bezpečnosti.
d. Ručí za trvalé zachování mlčenlivosti všech svých pracovníků i po ukončení smluvního vztahu s úřadem.

Dodavatel je povinen akceptovat použití prostředků bezpečnostního auditu, které mohou být útvarem IT využity k sledování aktivit v prostředí ICT/IS či aktivity procházejících přes toto prostředí.

A.2 Ochrana Aktiv

Dodavatel se před vlastním **přístupem** k datům a informacím KÚ JK musí zavázat mlčenlivostí. Tzn., že platí povinnost Dodavatele se zavázat a také povinnost pracovníků KÚ JK (prioritně ve smlouvě, prohlášením Dodavatele, formulářem, ...) zavázat Dodavatele a nezpřístupnit data a informace Dodavateli dříve, než dojde k jeho závazku mlčenlivosti (tj. podpisu NDA – Non Disclosure Agreement či CA – Confidentiality Agreement).

A.3 Přístup k ICT/IS

Přihlášení Dodavatele do sítě KÚ JK musí podléhat kontrole přístupu na základě autorizace po předchozí autentizaci, včetně autentizace přes VPN v případě užití VPN klienta. Přihlašovací proces do VPN a do Windows domény poskytuje základní bezpečnostní funkce – nikdy se nezobrazuje vkládané heslo a heslo není nikde přenášeno a ukládáno v nezašifrované formě. Přístup ke službám ICT/IS je vždy zajištěn přes proces autentizace, autorizace a bezpečnostního auditu.

A.4 Ochrana před škodlivým softwarem

Dodavatel je povinen:

a. Centrálně organizovat zabezpečení svých koncových stanic v připojeních do své infrastruktury (např. řízení personálních firewallů, antivirového SW atd.) a to minimálně na úrovni standardů KÚ JK. Standardy KÚ JK se řídí zákonem č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a zejména vyhláškou č. 82/2018 Sb. Vyhláška o kybernetické bezpečnosti a dále bezpečnostními doporučeními NCKB pro administrátory v aktuálně platné verzi. Dodavatel by měl v přiměřené míře splňovat požadavky uvedených dokumentů.
b. Obsahem antivirové ochrany jsou taková opatření technického a administrativního charakteru, která vedou k detekci a následnému odstranění infiltrujícího software u všech prostředků provozovaných v rámci infrastruktury Dodavatele.
c. Dodavatel musí na své straně definovat zásady bezpečného užívání Internetu a s těmito zásadami seznámit veškerý personál užívající ICT prostředky infrastruktury Dodavatele.
d. Dodavatel musí na pracovních stanicích v jeho odpovědnosti zajistit bezpečné nakonfigurování prohlížečů obsahu Internetu (např. www prohlížeče).

A.5 Řízení bezpečnostních rizik

Dodavatel je povinen zajistit, že:

a. Hesla pracovníků Dodavatele nebudou zaznamenávána v otevřené podobě.
b. Vzájemnou spolupráci a komunikaci mezi Dodavatelem a KÚ JK při řešení ICT bezpečnostní rizik

A.6 Hlášení

Dodavatel je povinen KÚ JK hlásit:

1. nestandardní situace při práci v ICT/IS;
2. bezpečnostní události nad ICT/IS;
3. bezpečnostní slabiny v ICT/IS Objednatele.

A.7 Kontrola a audit Dodavatele

KÚ JK má obecné právo auditu prostředí Dodavatele za účelem ověření dodržování Bezpečnostních pravidel Objednatele či za účelem ověření zabezpečení dat a informací na ICT prostředcích Dodavatele, a to minimálně 1x za 12 měsíců.

A.8 Ošetření výjimek

Ve výjimečných případech je možno vyhlásit výjimku z dodržování bezpečnostních pravidel. Udělení výjimek ze stanovených pravidel se provádí na základě požadavku zaslaného manažerovi kybernetické bezpečnosti, který má právo výjimku udělit.

Schváleno: Bezpečnostní komise – Výbor pro řízení kybernetické bezpečnosti