SMLOUVA O POSKYTNUTÍ SLUŽBY

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

mezi těmito smluvními stranami:

Objednatel:
Město Bučovice
IČ: 00291676
se sídlem: Jiráskova 502, 685 01 Bučovice
zastoupené: Mgr. Andreou Kovářovou, tajemnicí
(dále jen „Objednatel“)

a

Dodavatel:
IT Cluster, z. s.
IČO: 27021408
se sídlem: Novoveská 1139/22, Mariánské Hory, 709 00 Ostrava
zastoupen: Miroslavem Hamplem, předsedou výkonné rady
(dále jen „Dodavatel“)

Článek I. – Předmět smlouvy

1. Dodavatel se zavazuje provést pro Objednatele službu s názvem závěrečný audit kybernetické bezpečnosti, a to v souladu se svou nabídkou a požadavky Objednatele.
2. Objednatel se zavazuje za řádné a včasné poskytnutí služby zaplatit Dodavateli cenu ve výši 107 690 Kč včetně DPH.

Článek II. – Termín plnění

1. Dodavatel se zavazuje předat výstup služby nejpozději do 30.04.2026. Pokud by došlo v důsledku nedodržení ustanovení smlouvy ke krácení dotace, budou případné škody vymáhány po dodavateli.
2. Nedodá-li Dodavatel písemný výstup do 14 dnů po uplynutí lhůty dle čl. II odst. 1 této smlouvy, je Objednatel oprávněn od smlouvy odstoupit.

Článek III. – Mlčenlivost a důvěrnost informací

1. Dodavatel se zavazuje zachovávat mlčenlivost o všech informacích důvěrné povahy, které mu budou v rámci spolupráce sděleny nebo které jinak získá při plnění této smlouvy, zejména se

jedná o: topologii sítě, osobní údaje zaměstnanců, přístupová jména a hesla, technickou konfiguraci systémů a bezpečnostní opatření.

2. Povinnost mlčenlivosti trvá i po skončení této smlouvy.
3. Výjimkou z povinnosti mlčenlivosti je zákonná povinnost sdělení údajů orgánům veřejné moci, v takovém případě Dodavatel předem informuje Objednatele.

Článek IV. – Součinnost a odpovědnost

1. Objednatel se zavazuje poskytnout Dodavateli veškerou potřebnou součinnost nezbytnou pro řádné splnění předmětu smlouvy, zejména poskytnutím požadovaných podkladů a informací bez zbytečného odkladu.
2. V případě, že Objednatel neposkytne součinnost ani do 10 pracovních dnů od prokazatelné výzvy Dodavatele, je Dodavatel oprávněn od smlouvy odstoupit a požadovat úhradu prokazatelně vzniklých nákladů souvisejících s přípravou a částečnou realizací zakázky.

Článek V. – Závěrečná ustanovení

1. Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma stranami.
2. Nedílnou součástí této smlouvy jako příloha je zadávací dokumentace Objednatele.
3. Smlouva je uzavřena na dobu určitou do splnění všech povinností z ní vyplývajících.
4. Veškeré změny a doplnění této smlouvy mohou být činěny pouze písemně formou číslovaných dodatků podepsaných oběma stranami.
5. Právní vztahy touto smlouvou výslovně neupravené se řídí příslušnými ustanoveními občanského zákoníku.
6. Tato smlouva je vyhotovena ve dvou vyhotoveních, z nichž každá strana obdrží po jednom.

Za Objednatele:
Mgr. Andrea Kovářová

Za Dodavatele:
Miroslav Hampl

Příloha ke smlouvě – zadávací podmínky zadavatele

Předmět

Předmětem této výzvy je zpracování auditu kybernetické bezpečnosti v rámci projektu „**Bezpečný digitalizovaný úřad města Bučovice**“ (dále také jen „dílo“). Dílo bude realizováno v souladu s požadavky Výzvy č. 41 - Kybernetická bezpečnost – obce, Investice 3: Kybernetická bezpečnost, Národního plánu obnovy Ministerstva vnitra České republiky (dále jen „výzva č. 41“). Audit je součástí povinných výstupů projektu a musí být proveden kvalifikovaným auditorem dle platné legislativy.

Pro účely stanovení ceny jsou přílohami výzvy – příloha č. 2 vyplněná technická specifikace z veřejné zakázky „Pořízení a instalace prvků zvyšující kyberbezpečnost“ od vybraného dodavatele a příloha č. 3. Rozhodnutí o přidělení dotace vč. všech příloh (příloha č. 1 podmínky realizace, příloha č. 2. produktový rozpad).

Cílem bezpečnostního auditu je

- porovnání projektové dokumentace (dále jen „PD“) na vstupu s výstupy projektu, tj. zda realizace proběhla dle PD a posouzení, zda přispěla ke zvýšení kybernetické bezpečnosti definovaných informačních systémů,
- zodpovězení otázky, zda došlo k nasazení vybraných technologií a služeb dle předloženého projektu a zda došlo k posílení kybernetické bezpečnosti uvedených informačních systémů.

Audit bude proveden dle podmínek výzvy č. 41.

Požadavky na osobu provádějící audit (dále jen „auditor“) dle 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):

Praxe:

- alespoň 3 roky praxe v oblasti auditu informační nebo kybernetické bezpečnosti nebo
- absolvování studia na vysoké škole a alespoň 1 rok praxe v oblasti auditu informační nebo kybernetické bezpečnosti

Certifikace:

- Certified Information Systems Auditor (CISA),
- Certified Internal Auditor (CIA),
- Certified in Risk and Information Systems Control (CRISC),
- Lead Auditor Information Security Management Systém (Lead Auditor ISMS),
- Auditor BI (akreditační schéma ČIA)
- případně jiný než výše uvedený certifikát, jestliže bude splňovat požadavky ISO 17024 – Posuzování shody

Auditor musí být nezávislý na dodavateli řešení a nesmí být v konfliktu zájmů.

Rozsah činností auditu

Audit musí zahrnovat:

- Kontrolu souladu realizace projektu s právním aktem (Rozhodnutí o schválení finanční podpory)
- Posouzení posílení kybernetické bezpečnosti u vybraných informačních systémů
- Ověření splnění indikátorů a požadavků projektu
- Vyhotovení závěrečné zprávy z auditu
- Kontrola implementace vybraných opatření na místě
  - ověření implementace bezpečnostních opatření přímo na místě
  - praktické testování vybraných opatření
  - příprava záznamů zjištění z testování opatření na místě

Harmonogram auditu

Předpokládaný termín realizace auditu:

- Zahájení **do 5 dnů** od zveřejnění smlouvy v registru smluv. Termín ukončení auditu a předání závěrečné zprávy auditu do 30.04.2026.

Další požadavky na zpracování auditu

- Při realizaci projektu bude auditor vycházet z předmětu projektu a popsaného způsobu realizace, z rozpadu projektu na hlavní produkty, kde jsou žadatelem vždy stanoveny „posílené informační systémy v rámci zabezpečení kybernetické bezpečnosti“, názvy těchto vybraných informačních systémů (dále jen „IS“) i způsob, jakým má být u nich dosaženo posílení kybernetické bezpečnosti.
- Tím je dán základní rámec auditu, minimální požadovaný rozsah činností auditora, proto je nutné, aby auditor při posuzování také vycházel z těchto závazných dokumentů výzvy č. 41 a zahrnul do svého znaleckého posuzování jak vyjmenované IS, tak uvedené způsoby realizace.