OBJEDNÁVKA

Objednavatel

Státní investiční a rozvojová společnost, a.s.
zapsaná v OR: Městský soud v Praze, sp. zn. B 28761
se sídlem: Na Poříčí 1046/24, Nové Město, 110 00 Praha 1
[redacted]
IČO: 21333858, DIČ: CZ21333858

Dodavatel

Jakub Breckl
Se sídlem: Kolšov 163, 788 21 Kolšov
IČO: 22021825

Předmět, termín a místo plnění

Objednáváme Analýzu současného stavu, návrh a implementaci systému řízení aktiv a rizik, který bude plně odpovídat požadavkům zákona o kybernetické bezpečnosti a návrh opatření pro zvýšení celkové úrovně bezpečnosti a zajištění souladu s legislativou dle vaší nabídky ze dne 13.9.2024, která tvoří přílohu č. 2 této Objednávky. Předmětem je plnění viz Příloha č. 1 – Poptávka této Objednávky.

Výše uvedené plnění bude dodáno v termínu **do 6. 12. 2025**
Místo plnění je sídlo objednatele

Cena

Celková cena: 183.000,- bez DPH

Platební podmínky

Objednatel uhradí cenu na základě faktury, kterou dodavatel vystaví a zašle na e-mailovou adresu: [redacted] objednateli nejpozději do 10 (slovy: „deseti“) kalendářních dní po řádném plnění této objednávky, což bude stvrzeno podepsáním Akceptačního protokolu.
Příslušnou cenu uhradí objednatel formou bezhotovostního převodu na účet dodavatele uveden na faktuře. Faktura musí obsahovat odkaz na tuto Objednávku. Dále musí každá faktura obsahovat veškeré náležitosti daňového dokladu stanovené příslušnými právními předpisy, zejména zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a § 435 občanského zákoníku.

Splatnost faktury činí 30 (slovy: „třicet“) kalendářních dní a počítá se ode dne doručení faktury objednateli.
Nebude-li faktura splňovat veškeré výše uvedené náležitosti daňového dokladu, nebo bude-li mít jiné závady v obsahu, je objednatel oprávněn ji ve lhůtě její splatnosti dodavateli vrátit a dodavatel je povinen vystavit a doručit objednateli fakturu opravenou či doplněnou. V případě vrácení faktury dle předcházející věty se lhůta splatnosti přerušuje a nová lhůta splatnosti počíná běžet od počátku až dnem následujícím po dni, kdy byla opravená nebo doplněná faktura splňující všechny náležitosti dle příslušných právních předpisů a požadavky dle této smlouvy, doručena objednateli.

Smluvní pokuty

Při nedodržení výše stanoveného termínu dodání předmětu plnění Vám bude účtována smluvní pokuta ve výši 0,05% z ceny plnění za každý i započatý den prodlení.

Ostatní ujednání

Akceptací této objednávky dodavatel souhlasí se zveřejněním celého obsahu objednávky v registru smluv pro případ, že podléhá povinnosti zveřejnění ve smyslu zákona č. 340/2015 Sb., o registru smluv, a prohlašuje, že objednávka neobsahuje obchodní tajemství ani údaje, které by neměly být zveřejněny, s výjimkou údajů, které dle názoru objednatele naplňují výjimku z povinnosti zveřejnění dle zákona o registru smluv. Pro případ, že by dodavatel zjistil, že objednávka obsahuje obchodní tajemství popř. údaje, které dle právních předpisů nemají být zveřejněny, zavazuje se do tří dnů od obdržení objednávky předat objednateli kopii objednávky se začerněnými údaji, které nemají být zveřejněny, a s poskytnutím odůvodněním pro jejich nezveřejnění.

Přílohy:

a) Poptávka
b) Nabídka ze dne 13.09.2024

V Praze dne dle data el. podpisu

[redacted]

Ing. Petr Križan
místopředseda představenstva

Ing. David Petr
člen představenstva

Státní investiční a rozvojová společnost, a.s.
Na Poříčí 1046/24, budova A
110 00 Praha 1

info@sirsdevelopment.cz
www.sirsdevelopment.cz

Název poptávky:	**Zavedení systému řízení rizik kybernetické bezpečnosti – analýza rizik dle NIS2**
Poptávkové řízení:	Tato poptávka je poptávaná jako zakázka malého rozsahu mimo rámec zákona v souladu s ustanovením § 31 zákona č. 134/2016 Sb., o zadávaní veřejných zakázek (dále jen „ZZVZ“) a podle zásad § 6 ZZVZ.
Způsob zadání:	Uzavřená výzva
Zadavatel:	Státní investiční a rozvojová společnost Na Poříčí 1046/24, Nové Město, 110 00 Praha 1 IČO: 21333858
Předmět plnění:	Předmětem zakázky je posouzení aktuálního stavu a zavedení systému řízení aktiv a rizik v souladu s připravovaným zákonem o kybernetické bezpečnosti, který vychází ze směrnice EU o kybernetické bezpečnosti („NIS2“). Primárním cílem je získat rámcový přehled a vstupní informace, jak efektivně zavést a řídit systém řízení rizik s důrazem na realizaci analýzy rizik a návazných postupů a procesů včetně souvisejících metodik. **Plnění zakázky se bude skládat z následujících oblastí:** 1. Analýza současného stavu 2. Vytvoření systému řízení aktiv a rizik: návrh a implementace systému řízení aktiv a rizik, který bude plně odpovídat požadavkům připravovaného zákona o kybernetické bezpečnosti 3. Návrhy na vylepšení: Na základě provedené analýzy požadujeme návrh konkrétních opatření pro zajištění souladu s legislativou a zvýší celkovou úroveň bezpečnosti **Výstupem projektu bude zhotovení:** 1. metodiky řízení aktiv a rizik v oblasti kybernetické bezpečnosti, 2. katalogu hrozeb relevantních pro organizaci vycházející z novely zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších/nižších povinností, 3. metodiky hodnocení míry zranitelnosti v součinnosti s odpovědnými osobami organizace, 4. metodiky provedení analýzy rizik včetně identifikace primárních a podpůrných aktiv, 5. komplexní zhotovení analýzy rizik včetně postupu výpočtu hodnoty rizik a návazné kroky, které jsou uplatňovány v procesu řízení rizik (plán zvládání rizik, akceptace/přenesení/mitigace rizik), přičemž: a) Analýza rizik bude provedena kvalitativní metodou založenou na expertním odhadu hodnocení jednotlivých aktiv, který vyjadřuje hodnotu dopadu, hrozeb a zranitelností ve formě .xls souboru. b) Plán zvládání identifikovaných rizik obsahující doporučení pro optimalizaci nebo zavedení procesů, zavedení/úpravy bezpečnostní dokumentace či implementaci technických opatření pro snížení hodnot neakceptovatelných rizik na akceptovatelnou úroveň.

	Kontrolní mechanismus splnění jednotlivých kritérií bude proveden ověřením požadavků nového zákona o kybernetické bezpečnosti a souladu s jednotlivými výstupy.
Požadavky na prokázání kvalifikace a způsobilosti účastníka:	Podmínkou je, že zhotovitel musí mít: 1. Minimálně 2 roky praxi v oblasti kybernetické bezpečnosti. 2. Relevantní certifikát/školení z oblasti kybernetické bezpečnosti (např. manažer kybernetické bezpečnosti) 3. Osvědčení ISMS specialista, nebo ISMS manažer dle metodiky norem ČSN ISO/IEC 27001, ČSN ISO/IEC 27002 a zákona č. 181/2014 Sb.
Lhůta pro podání nabídek:	13. 09. 2024
Místo pro podání nabídek:	Nabídky zašlete na email kontaktní osoby: [redacted]
Předpokládaná hodnota:	200.000,- Kč bez DPH
Způsob zpracování nabídkové ceny:	Uvedení celkové nabídkové ceny za provedení díla
Kritéria pro výběr dodavatele:	Dodavatel bude vybrán dle výběrového kritéria ekonomické výhodnosti nabídky. Ekonomická výhodnost nabídky bude hodnocena podle nejnižší nabídkové ceny.
Hodnocení nabídek:	Výsledné pořadí nabídek bude stanoveno na základě nejnižší nabídkové ceny. Nabídky budou seřazeny dle nabídkových cen vzestupně, přičemž nejvýhodnější nabídkou bude nabídka s nejnižší nabídkovou cenou.
Přílohy:	

JAKUB BRECKL

Nabídka

Zavedení systému řízení rizik kybernetické bezpečnosti

Verze:	1.0
Datum:	13. 9. 2024
Připravil:	Ing. Jakub Breckl
Vypracováno pro:	Státní investiční a rozvojová společnost, a.s.

Obsah

1 Identifikační údaje

Jméno a příjmení	Jakub Breckl
Adresa:	Kolšov 163, 788 21 Kolšov
IČO:	22021825
Bankovní spojení:	[redacted]
Tel.:	[redacted]
Email:	[redacted]z
Zapsán v ŽV:	Úřad příslušný podle § 71 odst. 2 živnostenského zákona: Městský úřad Zábřeh

Nejsem plátce DPH.

2 Nabídka

Na základě zaslaného průzkumu trhu „Zavedení systému řízení rizik kybernetické bezpečnosti“ předkládám svou nabídku.

Předmětem nabídky je posouzení aktuálního stavu a zavedení systému řízení aktiv a rizik v souladu s připravovaným zákonem o kybernetické bezpečnosti, který se bude skládat z rámcového přehledu a informací, jak efektivně zavést a řídit systém řízení rizik vč. realizace analýzy rizik a návazných postupů, procesů a souvisejících metodik.

3 Cenová nabídka

Analýza současného stavu, návrh a implementace systému řízení aktiv a rizik, který bude plně odpovídat požadavkům připravovaného zákona o kybernetické bezpečnosti a návrh opatření pro zvýšení celkové úrovně bezpečnosti a zajištění souladu s legislativou.

Název projektu	**Cena celkem**
Zavedení systému řízení rizik kybernetické bezpečnosti	**183 000,- Kč**

Pozn. nejsem plátce DPH.

4 Certifikace a odborná způsobilost

- Oblasti kybernetické bezpečnosti jsem se intenzivně začal věnovat v roce 2021 v akademickém prostředí. Od roku 2022 se této problematice věnuji na profesní úrovni, kde se zaměřuji na implementaci a správu bezpečnostních opatření v rámci reálných projektů. Díky kombinaci akademického zázemí, praktických zkušeností a znalosti současné i nadcházející legislativy jsem schopen poskytnout komplexní řešení a odborný přístup v oblasti kybernetické bezpečnosti, zejména při zavádění a správě systému řízení bezpečnosti informací, s důrazem na nejnovější trendy a osvědčené postupy.
- Níže přikládám relevantní certifikace a osvědčení.

4.1 Manažer kybernetické bezpečnosti

- Certifikát získaný na základě prokázání a rozšíření klíčových aspektů řízení informační bezpečnosti napříč celým jejím životním cyklem, přenesení teoretických konceptů do praktického využití, aplikace postupů a metod odpovídajících místní legislativě i mezinárodním standardům, frameworkům a postupům.

4.2 ISMS manažer

- Osvědčení ISMS manažer potvrzuje odborné znalosti a dovednosti v oblasti zavádění, správy a udržování systému řízení bezpečnosti informací. Kurz zaměřen na identifikaci, hodnocení a řízení rizik spojených s ochranou citlivých informací, návrh a implementaci bezpečnostních opatření a zajištění souladu s platnou legislativou a bezpečnostními normami.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ

OSVĚDČENÍ

o úspěšném absolvování kurzu
s názvem

ISMS manažer

dle metodiky norem
ČSN ISO/IEC 27001, ČSN ISO/IEC 27002
a zákona č. 181/2014 Sb.

Breckl Jakub, Bc.

V Brně dne 2. 5. 2023

Ing. Petr Sedlák
Lektor

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ DĚKAN

doc. Ing. Vojtěch Bartoš, Ph.D.
Děkan FP VUT v Brně

Tento certifikát ověřuje úspěšné absolvování příslušného kurzu a byl vystaven pod evidenčním číslem: **ISMS-M-002/23**

4.3 ISMS specialista

- Osvědčení ISMS specialista potvrzuje odbornou způsobilost v oblasti systému řízení bezpečnosti informací v souladu s mezinárodními standardy a relevantní legislativou. Kurz zaměřen na prohloubení znalostí procesů, technik a metodik nezbytných pro implementaci, monitorování a udržování bezpečnostních opatření a na identifikaci rizik, návrh opatření ke zmírnění těchto rizik a zajištění, že systém řízení bezpečnosti informací splňuje požadavky dané normy a organizační potřeby.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ

OSVĚDČENÍ

o úspěšném absolvování kurzu
s názvem

ISMS specialista

dle metodiky norem
ČSN ISO/IEC 27001, ČSN ISO/IEC 27002
a zákona č. 181/2014 Sb.

Breckl Jakub, Bc.

V Brně dne 2. 5. 2023

Ing. Petr Sedlák
Lektor

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ DĚKAN

doc. Ing. Vojtěch Bartoš, Ph.D.
Děkan FP VUT v Brně

Tento certifikát ověřuje úspěšné absolvování příslušného kurzu a byl vystaven pod evidenčním číslem: **ISMS-S-003/23**