ALEF

Trust the Strong

Nabídka na srovnávací analýzu souladu se ZKB

Obsah

1 Úvod 3
1.1 Účel dokumentu 3
1.2 Dodavatel 3
1.3 Zástupce Dodavatele 3
1.4 Platnost nabídky 3
2 Informace o Dodavateli 4
2.1 Profil společnosti 4
2.2 Produktové certifikace ALEF NULA a.s. 5
3 Shrnutí požadavků Zákazníka 6
4 Popis navrženého řešení 7
4.1 Základní parametry projektu 7
4.2 Popisy klíčových produktů 12
4.2.1 Přezkoumání ISMS 12
4.2.2 Popis průběhu přezkoumání ISMS a technických opatřeních 13
4.4 Harmonogram 15
5 Reference bezpečnostních projektů 16
5.1 Implementace bezpečnostních systémů 16
5.2 Bezpečnostní služby a poradenství 16
6 Cenová nabídka 17
6.1 Rozpis ceny 17
6.2 Platební podmínky 17

1 Úvod

1.1 Účel dokumentu

Tento dokument obsahuje nabídku na provedení analýzy a zpracování dokumentace požadované zadavatelem, vztahující se ke splnění povinností zadavatele vyplývajících ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, v platném znění a souvisejících obecně závazných předpisů českého právního řádu.

Název společnosti:	**Správa úložišť radioaktivních odpadů**
Sídlo:	Dlážděná 6, 110 00 Praha 1
IČ:	66000769

1.2 Dodavatel

Název společnosti:	**ALEF NULA, a.s. (dále Dodavatel)** společnost je zapsaná v obchodním rejstříku Městského soudu v Praze, oddíl B., vložka 2727
Sídlo:	Pernerova 691/42, 186 00 Praha 8
IČ:	61858579
DIČ:	CZ61858579
Bankovní spojení:	Komerční banka, a.s.
č. účtu:	51-3717150237/0100
Jednající:	Milan Zinek, předseda představenstva
Telefon:	+420 225 090 111
Fax:	+420 225 090 112

1.3 Zástupce Dodavatele

Jména a příjmení:	xxxxx xxxxxxxxx
Telefon:	+420 xxx xxx xxx
E-mail:	xxxxxxxxxxxxxx@alef.com

1.4 Platnost nabídky

Tato nabídka je platná do 31. října 2021

2 Informace o Dodavateli

2.1 Profil společnosti

Společnost ALEF NULA a.s. je předním dodavatelem zákaznických řešení pro komunikační infrastrukturu v České republice a je součástí nadnárodní skupiny Alef Group, působící v několika zemích střední Evropy. Nejvyšší prioritou společnosti je dlouhodobá spokojenost zákazníků - tedy pozorné vnímání jejich potřeb a realizace řešení v nejvyšší kvalitě. I proto se ALEF NULA a.s. už od svého založení v roce 1994 orientuje na produkty renomovaných výrobců, především společnosti Cisco Systems. V této souvislosti je ALEF NULA a.s. držitelem nejvyšší partnerské certifikace Cisco Systems Partner – Gold Certified.
Kromě implementačních projektů tradiční LAN/WAN infrastruktury má ALEF NULA a.s. špičkové know-how, rozsáhlé zkušenosti i odborné certifikace v řadě dalších produktových oblastí – od datových center, přes síťovou bezpečnost a wireless až po IP telefonii, videokonferenční řešení a kontaktní centra. K tomu poskytuje ALEF NULA svým zákazníkům i konzultační služby, rychlou servisní podporu a školení. ALEF NULA je držitelem certifikace Cisco Learning Partner a patří mezi pět největších školicích středisek technologie Cisco v Evropě.
Systém řízení jakosti ALEF NULA, a.s. je ve shodě s normou ISO 9001:2008. ALEF NULA, a.s. má nastaveny vysoké standardy řízení bezpečnosti informací v souladu s normou ISO 27001:2013 a je držitelem bezpečnostní prověrky NBÚ na stupeň Tajné a NATO Secret.

2.2 Produktové certifikace ALEF NULA a.s.

Níže jsou uvedeny vybrané certifikace společnosti ALEF NULA, a.s.

- Cisco Gold Certified Partner,
- Cisco Advanced Collaboration Architecture Specialized Partner,
- Cisco Advanced Data Center Architecture Specialized Partner,
- Cisco Advanced Enterprise Networks Architecture Specialized Partner,
- Cisco Advanced Security Architecture Specialized Partner,
- Cisco Advanced Service Provider Architecture Specialized Partner,
- Cisco Express Specialized Partner,
- Cisco Learning Partner,
- Cisco Solution Partner.
- 2Ring Partner,
- AWS Consulting Partner,
- AWS Solution Provider & Training Partner,
- ATECO Partner,
- Commvault Partner,
- F5 Authorized Training Center,
- Flowmon Gold Partner,
- Microsoft Gold Technology Partner,
- MobileIron Partner,
- NetApp Contract Delivery Partner,
- Sewio Certified Partner,
- SPLUNK Associate Partner,
- VMware Solution Provider – Enterprise Partner,
- ZOOM Gold Partner.

3 Shrnutí požadavků Zákazníka

Předmětem plnění je provedení analýzy a zpracování dokumentace požadované zadavatelem, vztahující se ke splnění povinností zadavatele vyplývajících ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, v platném znění a souvisejících obecně závazných předpisů českého právního řádu.

Výsledkem předmětu díla budou zejména dokumenty

- Posouzení implementovaných organizačních a technických opatření v IT prostředí SÚRAO
- Identifikace informačních aktiv
- Analýza bezpečnostních rizik ve vztahu k informačním aktivům
- Plán zvládání rizik
- Zpracování návrhu opatření pro eliminaci nebo zmírnění identifikovaných rizik, s odstupňováním podle míry rizika a s uvedením doporučeného časového rámce pro eliminaci nebo zmírnění rizik
- Prohlášení o aplikovatelnosti
- Předběžná rámcová finanční kalkulace (předběžný odhad nákladů) na realizaci nápravných opatření (doporučení)
- Návrh akčního plánu s doporučeným harmonogramem Specifikace minimálního rozsahu oblastí analýzy je uvedena v následujících ustanoveních a koresponduje s danou vyhláškou v aktuálním znění.

4 Popis navrženého řešení

4.1 Základní parametry projektu

Název projektu	SÚRAO – GAP analýza souladu se ZoKB
Účel projektu	Přezkoumání implementace systému řízení kybernetické bezpečnosti a technických opatření systému řízení kybernetické bezpečnosti dle požadavků zákona č. 181/2014 Sb., ve znění dalších změn zákona a souvisejících vyhlášek.
Složení *Klíčové části/produkty určující rozsah projektu (scope)*	**Organizační část - zhodnocení organizačních opatření implementovaných v IT prostředí SÚRAO:** **Bezpečnostní politika a bezpečnostní dokumentace** Identifikace a analýza bezpečnostní dokumentace a provozních směrnic a postupů Zjednodušená definice primárních aktiv a hodnocení aktiv (CIA) **Organizace bezpečnosti informací** Role a odpovědnosti Oddělení odpovědností Informační bezpečnost v projektech Mobilní zařízení a práce na dálku **Bezpečnost lidských zdrojů** Povědomí, vzdělávání a školení bezpečnosti informací **Řízení aktiv** Management řízení aktiv a evidence aktiv Vlastnictví aktiv Odpovědnost za aktiva Klasifikace aktiv a informací Použití aktiv a životní cyklus aktiv Řízení použití nosičů informací a médií Manipulace s médii

Řízení přístupu a přístupových práv

- Požadavky organizace na řízení přístupu
- Řízení přístupu uživatelů a jejich odpovědnost
- Řízení přístupu k systémům a aplikacím

Fyzická bezpečnost pracovišť a zařízení

- Bezpečné oblasti
- Fyzický perimetr
- Fyzická bezpečnost a kontrola vstupu
- Zařízení a fyzická bezpečnost

Bezpečnost provozu

- Provozní postupy a odpovědnosti
- Dokumentace provozních postupů
- Řízení změn
- Řízení rizik / Plán zvládání rizik
- Řízení kapacit
- Princip oddělení prostředí vývoje, testování a provozu
- Ochrana proti malwaru
- Zálohování
- Logování, zaznamenávání a monitorování událostí
- Ochrana logů, logy o činnosti administrátorů a operátorů
- Správa provozního softwaru
- Opatření k auditu informačních systémů

Bezpečnost komunikací a přenos dat

- Přenos a ochrana informací

Akvizice, vývoj a údržba informačních systémů

- Bezpečnostní požadavky informačních systémů
- Bezpečnost v procesech vývoje a podpory
- Politika bezpečného vývoje
- Postupy řízení změn systémů
- Data pro testování

Bezpečnost pro dodavatele a třetí strany

- Bezpečnost informací v dodavatelských vztazích
- Bezpečnostní požadavky v dohodách s dodavateli

Řízení dodávek služeb dodavatelů

Řízení a zvládání bezpečnostních incidentů

Řízení incidentů bezpečnosti informací, sběr, vyhodnocování, reakce a zlepšování procesu

Řízení kontinuity organizace

Plánování kontinuity bezpečnosti informací
Implementace kontinuity bezpečnosti informací
Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací
Dostupnost vybavení pro zpracování informací
Nástroj pro zajišťování úrovně dostupnosti informací

Technologie šifrování

Politika pro použití kryptografických opatření

Soulad s interními a externími právními požadavky

Identifikace odpovídající legislativy a smluvních požadavků
Ochrana záznamů
Soukromí a ochrana osobních údajů
Ochrana duševního vlastnictví

Přezkoumání bezpečnosti informací

Nezávislá přezkoumání bezpečnosti informací
Shoda s bezpečnostními politikami a normami
Přezkoumání technické shody

Technická část – posouzení stavu implementace technických opatření zavedených v prostředí SÚRAO

Identifikace a kontrola implementace technických opatření

Fyzická bezpečnost
Fyzický bezpečnostní perimetr

	Bezpečnost komunikačních sítí Správa a ověřování identit Ochrana před škodlivým kódem Nástroj pro ochranu integrity komunikačních sítí Nástroj pro ověřování identity uživatelů Nástroj pro řízení přístupových oprávnění Nástroj pro ochranu před škodlivým kóde Nástroj pro zaznamenávání činnosti informačních systémů, jejich uživatelů a administrátorů Nástroj pro detekci kybernetických bezpečnostních událostí Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí Aplikační bezpečnost Kryptografické prostředky Nástroj pro zajišťování úrovně dostupnosti informací Bezpečnost průmyslových, řídicích a obdobných specifických systémů **Správa bezpečnosti sítě** Bezpečnost síťových služeb Opatření a kontroly v sítích Princip oddělení v sítích / segmentace komunikační sítě **Řízení technických zranitelností** Testování zranitelností bude provedeno u primárních aktiv, a to v případě, že budou tyto informace nutné pro realizaci auditu. V rámci implementace nápravných opatření pro řízení zranitelností a rizik se provede jejich obecný návrh a vydefinují se priority pro jejich realizaci.
Out-of-Scope *Významné produkty, které explicitně nejsou součástí rozsahu projektu*	• BIA • Detailní analýza aktiv, které nemají přímou souvislost se ZoKB • Připomínkování a úprava dokumentace mimo rámec projektu • Vytváření metodik, směrnic nebo jakékoliv jiné dokumentace pro potřeby řízení ZoKB • Návrh a optimalizace bezpečnostních procesů a zpracování bezpečnostní dokumentace

	• Detailní kontrola konfigurací • Detailní penetrační a vulnerability testování celé infrastruktury a aplikací • Návrh bezpečnostních opatření v detailu určení přesného produktu nebo posuzování více produktů proti sobě, průzkum trhu, komunikace s potenciálními dodavateli Zadavatele o návrhu bezpečnostních opatřeních a jiné detailní práce bezpečnostního návrhu • Definice pravidel a implementace systémů na ochranu osobních údajů • Vyjednávání s Národním bezpečnostním úřadem • Implementace konktrétních nápravných opatření s vyjímkou jejich obecné definice a prioritizace implementace.

4.2 Popisy klíčových produktů

4.2.1 Přezkoumání ISMS

Název produktu	Základní přezkoumání ISMS a technických opatření., ve znění dalších změn zákona a souvisejících vyhlášek.
Účel produktu	Kontrolní činnost dle §3 odst 1g vyhlášky 82/2018 Sb.
Složení *Klíčové části produktu*	**Hodnocení prostředí organizace k požadavkům zákona č. 181/2014 Sb. ve znění dalších změn zákona a souvisejících vyhlášek.** Zdokumentování současného stavu • Identifikace a základní zhodnocení rozporu s požadavky ZKB
Odvození *Vstupní podklady a závislosti na jiných produktech*	Schůzky realizované s pracovníky Objednatele. Smlouva. Zákon o kybernetické bezpečnosti a související vyhlášky. Stávající bezpečnostní dokumentace. (např. směrnice a politiky řízení kvality, hlavní politika úřadu, bezpečnostní politika úřadu a provozní řád objektu (fyzická bezpečnost), vzorové konfigurace a auditní logy, …).
Formát a způsob prezentace	Dokument předaný Zákazníkovi.
Akceptační kriteria	Dokument obsahuje kompletní a oboustranně schválené výstupy auditu.
Akceptační postup	• Dodavatel ve spolupráci se Zákazníkem zpracuje dokument a zašle jej k připomínkování a akceptaci Zákazníkovi • Zákazník provede revizi dokumentu a předá případné připomínky. Pokud připomínky nebudou, pak dokument akceptuje. • V případě, že budou existovat připomínky, pak je Dodavatel zapracuje příp. společně se Zákazníkem najdou jejich vhodné řešení/vypořádání. • Zákazník dokument schválí a podepíše převzetí. Předání dokumentů: • Zpráva z přezkoumání ISMS - Pro každé opatření bude uveden popis aktuálního stavu - Bude provedeno obecné hodnocení z pohledu požadavků prováděcí vyhlášky 82/2018 Sb. - Obsahem zprávy jsou veškeré paragrafy obsažené v prováděcí vyhlášce ZKB - Organizace se zkoumá z pohledu: ○ organizační opatření ○ technických opatření • Souhrné hodnocení stavu ○ Přehledový Excel s výpočetní logikou, který bude hodnotit výsledek GAP analýzy pro: ▪ Výkonné role podílející s na projektu ▪ Manažerské role (s menší mírou detailu)

	○ nasmlouvaných dodavatelů. Dodavatel poskytuje součinnost pro definici rozsahu. • Prezentace výsledků přezkoumání ISMS pro role Zákazníka zapojené do projektu ○ Prezentace a diskuze obvykle v rozsahu 2-3 hodin • Prezentace výsledků přezkoumání ISMS a technických opatření pro vrcholový management (v případě zájmu) ○ Prezentace a diskuze v rozsahu podle požadavku vrcholového vedení.

4.2.2 Popis průběhu přezkoumání ISMS a technických opatřeních

Úvodní fáze	Úvodní fází je zaslání dokumentace ze strany Zákazníka. Zejména: • bezpečnostní a provozní politiky a směrnice • definice aktiv • analýza rizik • zápisy z řídícího výboru KB • plány kontinuity • organizační struktura • topologie sítě • technická, provozní a bezpečnostní dokumentace • komunikační matice na zodpovědné osoby na straně Zákazníka
Zahajovací workshop	Zde je předmětem: • seznámení se s obecným fungováním organizace • seznámení se s cíly a podstatou činnosti organizace. • předání informací ohledně členění IT, topologií a zodpovědností. • vydefinování majitelů a provozovatelů jednotlivých aktiv • vydefinování specializovaných workshopů podle technologií, aplikací, lokalit apod. ○ Zákazník přiřadí zodpovědné osoby za jejich stranu
Specializované workshopy	• pohovory s vlastníky aktiv (většinou non-IT osoby). Obvykle HR, finanční oddělení, top management … • pohovory s provozovateli aktiv (obvykle s IT oddělením). Do této části patří i externí dodavatelé. Dochází zde k identifikaci podrobných informací do závěrečné zprávy
Vypracovávání závěrečné zprávy	• na základě získaných informací dojde k sepsání draftu závěrečné zprávy, dochází k upřesňování některých vstupů se Zákazníkem a vytvoření výsledného dokumentu Zpráva z přezkoumání ISMS k akceptaci.

Závěrečná prezentace	Prezentace pro: • projektový tým Zákazníka • vrcholové vedení Zákazníka
Získávání informací	• je skrze diskuzi s vlastníky a provozovateli aktiv • v případě potřeby se některé informace kontrolně a detailněji ověřují • používá se vzorková metoda. Tzn. pokud je nutné prověřit konfiguraci aplikací, zařízení, koncových systémů ad., kdy jich je větší množství (např. WAN směrovače), tak se nekontroluje soulad všech zařízení, ale jenom určitého vzorku (např. 1 zařízení od každého modelu).
Nedostatečné vstupy	V případě, že v organizační části auditu jsou nedostatečné vstupy u definice aktiv, analýzy rizik, v plánu zvládání rizik atd. tak: • bude provedena orientační identifikace potřebných vstupních informací • v případě potřeby bude aplikován kvalifikovaný odhad Úroveň těchto kroků nejsou náhradou analýzy rizik, metodikou pro určování aktiv, mapování zavislostí primárních a podpůrných aktiv, plánem zvládání rizik atd. Kvalifikovaný odhad může být použit i v technické části auditu, pokud Zadavetel nebude schopen dodat potřebné vstupy.
Časová osa projektu	• zahájení projektu přípravné práce 5 kalendářních dní (etapa 1) • sběr vstupních informací 30 kalendářních dnů (etapa 2+3) • zpracovaní finální zprávy 14 kalendářních dnů (etapa 4) Časová osa platí v případě dodržení součinnosti ze strany Zadavatele.

Součinnost	• zajištění součinnosti vlastníků a provozovatelů aktiv a to včetně externích subjektů
	• aktivní účast na workshopech ze strany vlastníků a provozovatelů aktiv a to včetně externích subjektů, dle dohodnutého harmonogramu.
	• poskytnutí vstupů pro technické hodnocení. Neposkytnutí požadovaných informací může mít dopad na obsahovou kvalitu díla.
	• dodání dokumentace
	  ○ kompletní ISMS dokumentace
	  ○ kompletní dokumentace sloužící k naplnění požadavků ZKB
	  ○ technická a provozní dokumentaci k síťovým prvkům, serverům, aplikacím apod.
	  ○ zajištění všech požadovaných vstupních informací v úvodních 2 kalendářmích týdnech od zahájení přezkoumání ISMS.

4.4 Harmonogram

Etapa	Trvání	Náplň
Etapa 1	Do 5 pracovních dnů od účinnosti smlouvy	Zahájení projektu – příprava kickoff, domluvení projektových pravidel
Etapa 2	Do 15 pracovních dnů od ukončení Etapy 1	Organizační a procesní část včetně revize, případně vytvoření návrhu bezpečnostní dokumentace minimálně v rozsahu: • základní definice aktiv • analýzy rizik • plánu zvládání rizik • prohlášení o aplikovatelnosti
Etapa 3	Do 15 pracovních dnů od ukončení Etapy 2	Technická část, Identifikace technických aktiv
Etapa 4	Do 14 pracovních dnů od ukončení Etapy 3	Prezentace a předání zpracovaných výstupů

4.2.1 Termín možného startu projektu

Dle dohody. Předpokládáme listopad 2021.

5 Reference bezpečnostních projektů

5.1 Implementace bezpečnostních systémů

Vybrané implementace v oblasti řízení informační bezpečnosti ICT:

- Generální ředitelství cel
- Český hydrometeorologický ústav
- Krajský úřad Jihočeského kraje
- ČEZ Distribuce, a.s.
- Mero ČR a.s.
- NET4GAS, s.r.o.
- Krajská Nemocnice Liberec, a.s.
- Ad. …

5.2 Bezpečnostní služby a poradenství

Vybrané služby v oblasti bezpečnostního auditu, bezpečnostního designu a poradenství:

- Český hydrometeorologický ústav
- Komerční banka, a.s.
- ERA a.s.
- Energetický regulační úřad
- Moravskoslezský kraj
- Institut klinické a experimentální medicíny
- Krajský úřad Olomouckého kraje
- Krajský úřad Pardubického kraje
- Krajský úřad Ústeckého kraje
- Ministerstvo průmyslu a obchodu
- České dráhy
- Generální ředitelství cel
- Zdravotnická záchranná služba Jihomoravského kraje
- Ad. …

6 Cenová nabídka

6.1 Rozpis ceny

Celková cena za předmět nabídky je 483.000 Kč bez DPH.

6.2 Platební podmínky

Splatnost faktur je 30 dní.