

Příloha č. 2 zadávací dokumentace

Technická specifikace

Obsah

1. Předmět veřejné zakázky.....	1
2. Využití zdrojů zadavatele.....	1
3. Požadované licence.....	2
4. Realizace	2

1. Předmět veřejné zakázky

Předmětem plnění Veřejné zakázky bude **dodávka softwarových prostředků** pro realizaci systému **řízení informačních rizik** a zvládání bezpečnostních událostí dle **technické specifikace a požadavků na funkcionalitu nástroje** uvedené dále v této příloze.

Předmětem plnění Veřejné zakázky bude dodávka softwarových prostředků a poskytnutí všech potřebných softwarových licencí. Dále pak instalace a implementace systému **řízení informačních rizik** a zvládání bezpečnostních událostí ve shodě s požadavky:

- **zákona 264/2025 Sb.**, Zákon o kybernetické bezpečnosti (dále též **ZoKB**),
- vyhlášky **Vyhláška č. 409/2025 Sb.**, Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále též **VoKB**),
- **zákon 266/2025Sb.** Zákon o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře)
- **CER (Critical Entity Resilience)** – direktiva EU
- normy **ISO 27001**, resp. normy řízení rizik informační bezpečnosti **ISO/IEC 27005** a vše v aktuálně platné verzi.

2. Využití zdrojů zadavatele

Dodávané řešení musí být realizovatelné a provozovatelné na infrastruktuře Zadavatele jako **samostatné řešení** postavené na virtualizační platformě Zadavatele. Dodávané řešení musí obsahovat všechny nezbytné softwarové prostředky pro poskytování požadovaných služeb a nesmí sdílet tyto prostředky s jinými systémy Zadavatele.

Zadavatel výslovně uvádí, že umožní vytvoření struktury virtuálních serverů dle potřeb dodávaného řešení na virtualizační platformě **VMware vSphere 8**, včetně funkce VMware HA. Zadavatel dále poskytne licence operačního systému **Microsoft Windows Server 2022 DataCenter** dle požadavků navrženého řešení.

Žádné jiné softwarové prostředky Zadavatele nemohou být využity. Všechny ostatní softwarové prostředky, komponenty nebo licence, nutné pro zprovoznění řešení (např. databázové systémy aj.), poskytování požadovaných služeb a legální provoz dodávaného řešení na infrastruktuře Zadavatele musí být součástí dodávky řešení v rámci tohoto výběrového řízení.

3. Požadované licence

A. Softwarový nástroj pro řízení informačních rizik - typ a rozsah

Rozsah a počet poskytnutých licencí musí pokrýt bezpečnostní role dle aktuálního zákona o kybernetické bezpečnosti, a dále všechny administrátorské role pro správu celého systému či jeho dílčích částí a další role nezbytné pro jeho užití v organizaci. Požadované minimální licenční zajištění je následující:

- minimálně 2x licence pro administrátory celého systému jako celku,
- minimálně 2x licence pro bezpečnostní management řízení rizik a aktiv (např. Manažer kybernetické bezpečnosti a Auditora kybernetické bezpečnosti),
- minimálně 10x licencí pro řízení rizik v celém životním cyklu (od hodnocení až po systém jejich zvládání) pro určený soubor aktiv (též tzv. funkční celek),
- multilicence – licenčně neomezené pro nahlížení a úpravy vedení evidence a hodnocení rizik aktiv kybernetických informačních systémů dle ZoKB (tj. v úrovni dostupnosti, důvěrnosti a integrity), včetně řízení jejich vazeb, pro kontrolní účely a schvalování (např. pro garanty aktiv nebo garanty podnikových procesů,
- multilicenci - licenčně neomezený přístup ke grafickému prostředí popisu struktury podnikových procesů a vazeb na podpůrná aktiva ve smyslu ZoKB, včetně vazeb na vizualizace a hlášení bezpečnostních událostí a incidentů z primárních dohledových systémů organizace.

Tento výčet licencí je obecný a postihuje bezpečnostní role v oblasti **řízení informačních rizik** a zvládání bezpečnostních událostí tak, jak to vnímá Zadavatel. Struktura licencí je věcí Uchazeče, nesmí však omezit uvedený rozsah užití a administrace.

4. Realizace

Realizace systému **řízení informačních rizik** a zvládání bezpečnostních událostí bude provedena na prostředcích Zadavatele v datovém centru lokality Pardubice (Pardubická nemocnice).

Práce

Součástí plnění předmětu Veřejné zakázky jsou i tyto práce:

- a. všechny **práce** spojené s realizací díla, zejména pak:
 - vypracování vstupního prováděcího plánu projektu (dále jen **Implementační plán projektu**), vč. akceptačních procedur (nutných k provedení akceptace díla) a akceptačních protokolů,
 - provedení veškerých úkonů a činností nutných k tomu, aby software mohlo plnit sjednaný či obvyklý účel, zejména:
 - **instalaci** dodávaného SW vybavení na prostředky zadavatele (viz. **Využití zdrojů zadavatele**) ve struktuře schválené v Implementačním plánu projektu,
 - **implementaci a vstupní nastavení** dodávaného řešení. Vstupním nastavením se rozumí základní nastavení všech procesů realizovaných dodávaným systémem, zejména procesů spojených s:
 - prováděním rizikových analýz a hodnocením rizik,
 - vedením agend všech podpůrných aktiv (ve smyslu zákona o kybernetické bezpečnosti ZoKB),
 - nastavením vizualizačních schémat a pohledů,

- plánováním a zvládáním řešení bezpečnostních událostí a
- procesy provádění auditů stavu kybernetické bezpečnosti
- reportováním

tak, aby systém řízení informačních rizik a zvládání bezpečnostních událostí vytvořil jeden konzistentní funkční celek.

- nastavení jednotných **metodik** a **pracovních postupů**.

b. Specifické činnosti

- zpracování rizikové analýzy a dekompozice podpůrných a primárních aktiv v rozsahu základní analýzy dle ZoKB, včetně vizualizace vazeb
- zpracování podkladů pro interní audit kybernetické bezpečnosti
- zavedení procesů ZoKB a interního auditu do SW nástroje

c. Konzultační činnosti

- Konzultační služby a podpora drobného rozvoje systémů (součástí smlouvy Smlouva o poskytování servisních služeb) v rozsahu 10MD/ročně

d. všechny typy **školení** potřebné pro práci s dodávaným řešením, zahrnuje zejména:

- školení systémových administrátorů, klíčových uživatelů a pracovníků v manažerských pozicích v počtu dle nastavených a obsazených rolí - odhad: do 10 osob
Cíl školení: schopnost samostatné administrace, nastavování systému a zavádění další služeb/aktiv pracovníky Zadavatele

e. kompletní **dokumentaci** v elektronické podobě, nezbytné pro použití dodávaného softwarového řešení, která zahrnuje minimálně tuto dokumentaci:

- **Uživatelský manuál** - popisem uživatelských funkcí dodávaného softwarového nástroje
- Dokumentaci pro **administraci** dodávaného řešení
- **Implementační plán projektu:**
 - analytická část – návrh realizace Díla a časový harmonogram,
 - plán školení administrátorů a dalších uživatelů dle specifických rolí
 - finální popis implementace dodávaného řešení (skutečné provedení),
 - akceptační procedury,
 - akceptační protokoly.
- **Exit plán** – plán o řízeném ukončení spolupráce,