3. CENOVÁ NABÍDKA ÚČASTNÍKA

Níže uvedená nabídková cena je stanovena jako cena smluvní se započtením veškerých nákladů, rizik, zisku a finančních vlivů (např. inflace) po dobu realizace zakázky v souladu s podmínkami uvedenými v zadávací dokumentaci.

Tab. 1: Cena

Název dodávky	Cena v Kč bez DPH	DPH v Kč	Cena v Kč včetně DPH
Provedení bezpečnostního auditu v oblasti kybernetické bezpečnosti v KVOP	199 000,-	41 790,-	240 790,-

Nabídková cena zahrnuje veškeré dodávky a činnosti vyplývající ze zadávacích podkladů vč. dopravy.

Platební a fakturační podmínky budou dohodnuty v objednávce nebo ve smlouvě.

Provedení bezpečnostního auditu je způsobilým výdajem v rámci případného projektu kybernetické bezpečnosti dle výzvy IROP.

4. DOBA A MÍSTO PLNĚNÍ

Provedení auditu a vypracování závěrečné zprávy proběhne do 4 měsíců od zahájeni (obdržení objednávky/podpisu smlouvy).

Místem plnění je Kancelář veřejného ochránce práv, Údolní 39, 602 00 Brno.

5. PŘEDMĚT NABÍDKY

Předmětem nabídky je provedení bezpečnostního auditu stavu technických a organizačních opatření v oblasti kybernetické bezpečnosti, dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů a vyhlášky 82/20018 sb. o kybernetické bezpečnosti v platném znění (dále jen VyKB) a také vybraných opatření dle normy ČSN EN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.

5.1. Provedení bezpečnostního auditu v oblasti kybernetické bezpečnosti

Bezpečnostní audit kybernetické bezpečnosti bude proveden v jednotlivých oblastech opatření dle ZKB a VyKB.

Oblasti technických opatření:

1. fyzická bezpečnost (§ 17 VyKB);
2. bezpečnost komunikačních sítí (§ 18 VyKB);
3. správa a ověřování identit (§ 19 VyKB);
4. řízení přístupových oprávnění (§ 20 VyKB);
5. ochrana před škodlivým kódem (§ 21 VyKB);
6. zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů (§ 22 VyKB);
7. detekce kybernetických bezpečnostních událostí (§ 23 VyKB);
8. sběr a vyhodnocení kybernetických bezpečnostních událostí (§ 24 VyKB);
9. aplikační bezpečnost (§ 25 VyKB);
10. kryptografické prostředky (§ 26 VyKB);
11. zajišťování úrovně dostupnosti informací (§ 27 VyKB).

Oblasti organizačních opatření:

1. systém řízení bezpečnosti informací (§ 3 VyKB)

2. řízení aktiv (§4 VyKB)
3. řízení rizik (§5 VyKB)
4. organizační bezpečnost (§6 VyKB)
5. bezpečnostní role (§7 VyKB)
6. řízení dodavatelů (§8 VyKB)
7. bezpečnost lidských zdrojů (§9 VyKB)
8. řízení provozu a komunikací (§10 VyKB)
9. řízení změn (§11 VyKB)
10. řízení přístupů (§12 VyKB)
11. akvizice, vývoj a údržba (§13 VyKB)
12. zvládání kybernetických bezpečnostních událostí a incidentů (§14 VyKB)
13. řízení kontinuity činností (§15 VyKB)
14. audit kybernetické bezpečnosti (§16 VyKB)
15. bezpečnostní politika a bezpečnostní dokumentace (§30 VyKB)

Bezpečnostní audit bude proveden formou dotazování a zaznamenávání odpovědí pracovníků organizace a fyzickým auditem na místě, za účelem zjištění, jaký je stav v jednotlivých oblastech technických a organizačních opatření.

Výsledkem bezpečnostního auditu bude „**Zpráva z bezpečnostního auditu v oblasti kybernetické bezpečnosti**", ve které budou uvedena zjištění z bezpečnostního auditu, vyhodnocení zjištění (tj. připomínky; požadavky na zlepšení; neshody; pozitivní zjištění) současného stavu opatření a dále budou identifikovaná významná rizika a příležitosti v oblasti kybernetické bezpečnosti.

5.2. Použití výsledků auditu

Dokument „Zpráva z bezpečnostního auditu v oblasti kybernetické bezpečnosti" může být také použit jako podklady pro případné vypracování studie proveditelnosti v oblasti zlepšení kybernetické bezpečnosti nebo jiné oblasti ICT v rámci projektu IROP.

6. POPIS POSKYTOVANÝCH SLUŽEB

Popis poskytovaných služeb je uveden na https://www.ajl.cz.