Veřejná zakázka

**„Zvýšení kybernetické bezpečnosti města Pelhřimov – část C“**

**Zadavatel:**

 **Město Pelhřimov**se sídlem Pelhřimov, Masarykovo náměstí 1, PSČ 393 01
IČO: 00248801
DIČ: CZ00248801

Osoba zastupující zadavatele: Ladislav Med, starosta

Detailní specifikace předmětu plnění

Předmětem plnění části C veřejné zakázky je provedení **nezávislého závěrečného auditu kybernetické bezpečnosti** města Pelhřimov po implementaci technických a organizačních opatření realizovaných v rámci části B (Infrastruktura) projektu **„Zvýšení kybernetické bezpečnosti města Pelhřimov“**, podpořeného z **Národního plánu obnovy (NPO)**, výzvy č. 41 – Kybernetická bezpečnost – obce.

Audit navazuje na výstupy části A (vstupní audit, GAP analýza a penetrační testy) a ověřuje, zda byla přijatá opatření účinná a vedla k prokazatelnému zvýšení úrovně bezpečnosti.

**Cíl části C ve vztahu k dotaci:**

Hlavním cílem je **nezávislé posouzení skutečného zvýšení kybernetické bezpečnosti** vybraných informačních a komunikačních systémů města a ověření souladu stávajícího bezpečnostního rámce s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a vyhlášky č. 82/2018 Sb., zejména § 18 a § 20.

Auditní výstupy budou sloužit jako podklad pro **doložení naplnění cílů a indikátorů dotační podpory**.

**Rozsah auditu:**

Závěrečný audit bude zaměřen na následující IKS města Pelhřimov:

1. **IS FENIX** – ekonomické a správní agendy
2. **IS EZOP** – elektronická spisová služba
3. **IS FLUXPAM 5** – mzdový a personální systém
4. **IS Elektronická pošta** – groupware a e-mailová komunikace
5. **IS Portál občana** – bezpečný přístup občanů ke službám města
6. **IS Doménové prostředí Windows serveru** – Active Directory, autentizační a autorizační služby

**Hlavní výstupy části C:**

1. **Závěrečný auditní protokol**, který bude obsahovat:
	* přehled realizovaných opatření v části B a jejich posouzení z hlediska dopadu na bezpečnost,
	* hodnocení souladu stavu informačních systémů se zákonem č. 181/2014 Sb., vyhláškou č. 82/2018 Sb. a doporučeními NÚKIB,
	* matice souladu „opatření (část B) → ověření (část C)
	* identifikaci případných reziduálních rizik a doporučení pro další zlepšení.
2. **Ověřovací penetrační testy**:
	* Zhotovitel provede cílené penetrační testy zaměřené na systémy, které prošly změnami nebo posílením v rámci části B, s cílem vyhodnotit aktuální úroveň bezpečnosti po realizaci části B
	* testy ověří odstranění dříve identifikovaných zranitelností z části A a zhodnotí, zda nedošlo k vytvoření nových zranitelných míst,
	* výstupem bude technická zpráva s přehledem provedených testů, identifikovaných slabin a doporučeními, doplněná přehledovou tabulkou „stav před vs. stav po“.
3. **Akceptační protokol (certifikát)** potvrzující:
	* že výstupy projektu vedly ke zlepšení úrovně kybernetické bezpečnosti města,
	* že byly splněny požadavky zákonné a dotační dokumentace,
	* že informační systémy dosáhly požadované míry odolnosti.
4. **Analýza rizik a zranitelností** – aktualizovaný dokument reflektující nový bezpečnostní stav.
5. **Dokumentace ISMS** dle doporučení NÚKIB, v rozsahu:
	* Politika kybernetické bezpečnosti
	* Katalog aktiv a hodnocení rizik
	* Role a odpovědnosti
	* Postupy řízení incidentů
	* Havarijní plán / plán obnovy
6. Dodavatel zpracuje pro každý auditovaný informační a komunikační systém (IKS) samostatný kontrolní checklist dle § 18 a § 20 vyhlášky č. 82/2018 Sb. pro každé z vybraných informačních systémů, který bude sloužit jako přehledné a auditovatelné ověření, zda jsou u konkrétního systému naplněny požadavky vyplývající z:
	* § 18 – Řízení aktiv
	(např. identifikace aktiv, přiřazení vlastníků, klasifikace aktiv, ochrana přístupů, evidence životního cyklu aktiv),
	* § 20 – Hlášení a řízení kybernetických bezpečnostních incidentů
	(např. postupy pro detekci, hlášení, reakci na incidenty, vedení evidence, eskalační mechanismy, povinnosti vůči NÚKIB apod.).

Checklist bude zpracován pro každý z výše vyjmenovaných IKS systémů a bude obsahovat u každého požadavku:

* + referenci na konkrétní odstavec vyhlášky (§, odst., bod),
	+ stav naplnění (Splněno / Částečně splněno / Nesplněno),
	+ odkaz na dokumentaci nebo důkaz (např. směrnice, logy, konfigurace, seznam aktiv),
	+ doporučení k nápravě nebo zlepšení (je-li relevantní).
	+ Checklist bude přiložen jako příloha závěrečného auditního protokolu a zároveň předán i v editovatelné podobě pro další interní využití městem

**Forma předání výstupů:**

* Výstupy budou zpracovány v **českém jazyce**, v elektronické i listinné podobě.
* Elektronická verze bude dodána ve formátu **PDF a DOCX/ODT**, auditní protokoly budou podepsány autorizovaným auditorem.
* Součástí bude i stručné **shrnutí závěrů pro účely dotačního monitoringu**.