Příloha č. 1 – cenová nabídka

CENOVÁ NABÍDKA

1. Cenová nabídka

Cenová nabídka za realizaci veřejné zakázky malého rozsahu „Zpracování bezpečnostní politiky systémů":

Cena díla bez DPH	DPH ve výši 21 %	Cena díla včetně DPH
518 000 Kč	108 780 Kč	626 780 Kč

Nabídková cena je uvedena jako absolutní a nepřekročitelná částka za provedení celkové zakázky a obsahuje veškeré náklady se zakázkou spojené.

2. Specifikace prováděných prací

I ÚVOD

Přístup k realizaci projektu chápeme tak, že zpracované dokumenty musí vyhovovat požadavkům stanoveným v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve vyhlášce č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), a v normách řady ISO 27000.

Výsledná dokumentace bude přizpůsobena organizaci tak, aby popisované procesy a role odpovídaly organizačnímu členění až na jednotlivé tabulkové pozice. V dokumentaci budou uvedeny odkazy na související akty řízení.

Součástí výstupu bude také doporučení na případné dopracování a sjednocení další bezpečnostní dokumentace OIPIT.

Při akceptaci každé důležité etapy projektu se předpokládá prezentace výstupů a oponentní řízení k předkládaným návrhům výstupů. Vždy bude brán ohled na požadavky zadavatele tak, aby výsledná dokumentace odpovídala jeho podmínkám a požadavkům.

II AKTUALIZACE BEZPEČNOSTNÍ POLITIKY OIPIT

II.1 Vstupní analýza OIPIT

1) Provede se posouzení vnitřního a vnějšího kontextu OIPIT.

    a. Identifikují se požadavky předpisů – zákonných a podzákonných - vždy v platném znění (zákon 273/2008 Sb., zákon 181/2014 Sb., zákon 101/2000 Sb., vyhláška 316/2014 Sb. atd.).

b. Identifikují se požadavky resortních předpisů (normativních aktů a příkazů Policejního presidenta a Ministra vnitra ČR a závazné bezpečnostní politiky nadřízených subjektů, které mají vztah k OIPIT).
c. Identifikují se případné smluvní závazky a další povinnosti, které mohou mít vliv na Bezpečnostní politiku OIPIT.
d. Identifikují se další závazky (služby), které OIPIT poskytuje, směrem k PČR a případně k MV, nebo které nakupuje od externích dodavatelů.
e. Provede se GAP analýza stávající Bezpečnostní politiky OIPIT, která ukáže, co v BP OIPIT není řešeno a co se musí změnit, nebo doplnit.

Výsledkem činností uvedených v bodech a. až d. bude tabulka požadavků na BP OIPIT.

2) Z výše uvedených analýz se provede stanovení kontextu organizace a stanovení rozsahu Bezpečnostní politiky OIPIT a působnosti OIPIT v oblasti řízení bezpečnosti informací.

II.2 **Posouzení rizik**

Na základě stanoveného rozsahu bezpečnostní politiky OIPIT budou stanovena primární aktiva OIPIT a typová podpůrná aktiva. Posouzení rizik bude provedeno podle metodiky standardu ČSN ISO 27005, kde bude použit přístup k posouzení rizik bezpečnosti informací E. 1 Přehledové posouzení rizik bezpečnosti informací.

Výsledkem posouzení rizik bude stanovení konkrétních parciálních rizik pro jednotlivá aktiva a vybrané hrozby.

Druhým výstupem analýzy rizik bude stanovení účinnosti jednotlivých opatření dle přílohy „A" standardu ISO 27001. Pro použití v podmínkách zákona o kybernetické bezpečnosti budou jednotlivá opatření standardu ISMS namapována na opatření vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti.

II.3 **Presentace výsledků Vstupní analýzy OIPIT**

Proběhne presentace výsledků Vstupní analýzy OIPIT, Posouzení rizik, návrhu přístupu k řízení bezpečnosti informací a obsahu Bezpečnostní politiky OIPIT, které budou diskutovány a podle požadavků zadavatele upraveny.

II.4 **Aktualizace bezpečnostní politiky OIPIT**

Na základě schválených výsledků vstupní analýzy OIPIT proběhne aktualizace dokumentu bezpečnostní politika OIPIT. Dokument se předloží zadavateli k připomínkám a proběhne oponentní řízení, během kterého budou zapracovány požadavky zadavatele. Dokument se zapracovanými připomínkami se předloží vedení zadavatele k akceptaci.

III **PROVÁDĚCÍ BEZPEČNOSTNÍ SMĚRNICE**

Prováděcí bezpečnostní směrnice bude rozvíjet bezpečnostní politiku OIPIT do konkrétních procesů. Již při tvorbě Bezpečnostní politiky OIPIT budou definovány konkrétní procesy, kterými se politika realizuje. Tyto procesy budou detailně popsány v Prováděcí bezpečnostní směrnici.

Prováděcí bezpečnostní směrnice bude specifikovat jednotlivé procesy, určí jejich vlastníky a odpovědné osoby za jejich realizaci, provozování, kontrolu a měření a vyhodnocování.

IV STRATEGIE ŘÍZENÍ KONTINUITY ČINNOSTI DATABÁZOVÉHO CENTRA POLICIE ČR

Strategie řízení kontinuity činnosti Databázového centra bude založena na provedení analýzy dopadů (BIA, Business Impact Analysis).

V rámci analýzy dopadů budou identifikována aktiva významná pro provoz databázového centra. Tato aktiva budou ohodnocena z hlediska požadavků na dostupnost a maximální tolerovatelné doby výpadku aktiva. Budou identifikovány vzájemné závislosti mezi aktivy a bude vypočítán požadovaný čas obnovy jednotlivých aktiv. Za časů obnovy bude definováno pořadí obnovy jednotlivých aktiv.

Budou rozebrány případy, kdy reálný čas obnovení aktiva bude delší než maximální tolerovatelný čas výpadku aktiva. V těchto případech bude buďto doporučeno technické řešení nápravy, nebo redundance prostředků.

V rámci strategie řízení kontinuity databázového centra budou vybrány nejpravděpodobnější scénáře ohrožení činností centra a tyto scénáře budou vyhodnoceny z hlediska možných dopadů na činnost databázového centra.

Na základě posouzení aktuálního stavu, bude navržena struktura managementu pro řízení kontinuity databázového centra. Budou popsány role a aktivity, které role v rámci řízení kontinuity činnosti budou provádět.

V rámci strategie řízení kontinuity činnosti databázového centra bude také popsána struktura plánů kontinuity.

V TYPOVÁ BEZPEČNOSTNÍ DOKUMENTACE INFORMAČNÍHO SYSTÉMU

Typová bezpečnostní dokumentace systému bude svojí strukturou vycházet z přílohy č. 4 k vyhlášce č. 316/2014 Sb., a z ustanovení bezpečnostní politiky OIPIT.

V.1 Typová bezpečnostní politika systému

Bude zpracována typová bezpečnostní politika systému, která bude obsahovat bezpečnostní politiky z vyhlášky č.316/2014 Sb., které budou uvedeny ve formě jednotlivých kapitol. Typová bezpečnostní politika bude obsahovat následující kapitoly:

1) Politika systému řízení bezpečnosti informací,
2) Politika organizační bezpečnosti,
3) Politika řízení dodavatelů,
4) Politika klasifikace aktiv,
5) Politika bezpečnosti lidských zdrojů,
6) Politika řízení provozu komunikací,
7) Politika řízení přístupu,
8) Politika bezpečného chování uživatelů,
9) Politika zálohování a obnovy,
10) Politika bezpečného předávání a výměny informací,
11) Politika řízení technických zranitelností,
12) Politika bezpečného používání mobilních zařízení,
13) Politika poskytování a nabývání licencí programového vybavení a informací,
14) Politika ochrany osobních údajů,
15) Politika fyzické bezpečnosti,
16) Politika bezpečnosti komunikační sítě,

17) Politika ochrany před škodlivým kódem,
18) Politika nasazení a používání nástroje pro detekci chyb a kybernetických bezpečnostních událostí,
19) Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
20) Politika bezpečného používání kryptografických ochrany.

V rámci této politiky, tam, kde je to použitelné, budou přednostně použity u OIPIT již zavedené procesy a postupy. V případech, kdy postupy zavedené OIPIT budou v rozporu se vyhláškou č. 316/2014 Sb., budou v politice upřednostněny přístupy definované touto vyhláškou.

Obsah jednotlivých politik bude vycházet z vyhlášky o kybernetické bezpečnosti a v rámci detailních postupů budou použity popisy bezpečnostních opatření ze standardu ISO IEC 27002.

V.2 **Další dokumentace**

Další dokumentace bude, stejně jako bezpečnostní politika, svojí strukturou vycházet z přílohy č. 4 k vyhlášce č. 316/2014 Sb., a z ustanovení bezpečnostní politiky OIPIT.

Bude zpracována následující typová dokumentace:

1) Zpráva z auditu kybernetické bezpečnosti (vzor dokumentu),
2) Zpráva z přezkoumání systému řízení bezpečnosti informací (vzor dokumentu),
3) Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik (popis metodiky),
4) Zpráva ohodnocení aktiv a rizik (vzor dokumentu),
5) Prohlášení o aplikovatelnosti (vzor dokumentu),
6) Plán zvládání rizik (vzor dokumentu),
7) Plán rozvoje bezpečnostního povědomí (vzor dokumentu),
8) Zvládání kybernetické bezpečnostních incidentů (typový dokument popisující zásady a procesy, který musí být upřesněn pro konkrétní informační systém),
9) Strategie řízení o kontinuity činnosti (typový dokument popisující zásady a procesy, který musí být upřesněn pro konkrétní informační systém),
10) Přehled obecně závazných právních předpisů vnitřních předpisů jiných předpisů smluvních závazků (přehled aktuálně platných dokumentů).

I v případě těchto dokumentů budou upřednostňovány již zavedené postupy u OIPIT, pokud nebudou v rozporu s vyhláškou o kybernetické bezpečnosti.

V.3 **Schvalování typové bezpečnostní dokumentace informačního systému**

Celá sada výše uvedených dokumentů bude podrobena oponentnímu řízení se zadavatelem, v rámci něhož budou projednány všechny připomínky a zapracovány úpravy do dokumentace tak, aby co nejdéle vyhověla požadavkům zadavatele.

VI **SMĚRNICE PRO PROVÁDĚNÍ INTERNÍCH AUDITŮ BEZPEČNOSTI INFORMACÍ**

Bude zpracována typová směrnice interních auditů bezpečnosti informací, která vychází s požadavků vyhlášky č. 316/2014 Sb., norem ISO 27001 a 19011. V typové směrnici budou stanovena základní pravidla pro prováděné činnosti při:

1) plánování,
2) provádění, a

3) vyhodnocování interních auditů bezpečnosti informací.

Budou stanoveny základní odpovědnosti a pravomoci pro jednotlivé role (manažera kybernetické bezpečnosti, vedoucího auditora a auditora) v rámci provádění interních auditů bezpečnosti informací. V dokumentu budou definovány požadavky na:

1) výběr,
2) kvalifikaci, a
3) výcvik auditora kybernetické bezpečnosti.

Součástí dokumentu budou vzory dokumentů zpracovávané při provádění interních auditů. Jedná se o tyto vzory:

1) Roční program auditů (vzor dokumentu),
2) Plán interního auditu (vzor dokumentu),
3) Zpráva z auditu kybernetické bezpečnosti (vzor dokumentu).

I v případě tohoto dokumentu budou upřednostňovány již zavedené postupy u OIPIT, pokud nebudou v rozporu s vyhláškou o kybernetické bezpečnosti.

VII **SMĚRNICE PRO TESTOVÁNÍ BEZPEČNOSTI**

Bude zpracována typová směrnice pro testování bezpečnosti informačních systémů, která bude stanovovat základní pravidla pro plánování testování bezpečnosti, použití testovacích metod, jejich vyhodnocování a stanovení výstupů vyhodnocení testování bezpečnosti.

Budou stanovena pravidla a odpovědnosti pro přijímání opatření na základě výsledků testování bezpečnosti informačních systémů.

V dokumentu budou dále stanoveny základní odpovědnosti a pravomoci pro jednotlivé role v rámci testování bezpečnosti.

I v případě tohoto dokumentu budou upřednostňovány již zavedené postupy u OIPIT, pokud nebudou v rozporu s vyhláškou o kybernetické bezpečnosti.

VIII **SMĚRNICE PRO SPRÁVU A ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ**

Bude zpracována typová směrnice pro správu a zvládání bezpečnostních incidentů, která bude popisovat základní pravidla a odpovědnosti v rámci řízení bezpečnostních událostí a incidentů. Jednotlivá pravidla budou zpracována v souladu s požadavky vyhlášky č. 316/2014 Sb.

V dokumentu budou definovány jednotlivé kroky při zvládání bezpečnostních událostí a incidentů, aktivace týmu pro řešení kybernetických bezpečnostních událostí, dále pravidla pro komunikaci s Národním bezpečnostním úřadem a reakci na opatření vydané tímto NBÚ.

Dokument bude obsahovat stanovení rolí, pravomocí a odpovědností v rámci řešení bezpečnostních událostí a incidentů.

I v případě tohoto dokumentu budou upřednostňovány již zavedené postupy u OIPIT, pokud nebudou v rozporu s vyhláškou o kybernetické bezpečnosti.

IX **SMĚRNICE PRO ZÁLOHOVÁNÍ, OBNOVU A TESTOVÁNÍ OBNOVY**

Bude zpracována typová směrnice pro zálohování, obnovu a testování obnovy vycházející z politiky kontinuity činností.

Dokument bude stanovovat základní pravidla pro tvorbu:

1) plánu zálohování,
2) havarijních plánů, a
3) plánů obnovy.

V dokumentu budou dále stanoveny odpovědnosti jednotlivých rolí při tvorbě plánů.

Součástí dokumentu budou vzory dokumentů. Jedná se o tyto vzory:

1) Plán zálohování (vzor dokumentu),
2) Havarijní plán a plán obnovy (vzor dokumentu).

I v případě tohoto dokumentu budou upřednostňovány již zavedené postupy u OIPIT, pokud nebudou v rozporu s vyhláškou o kybernetické bezpečnosti.