Opis predmetu zákazky

1. Názov projektu

Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS

2. Všeobecný popis zadania

Hlavným výsledkom realizácie projektu je zavedenie procesov governance IT bezpečnosti a riadenia rizík do našej organizácie. Vedľajším produktom je samozrejme aj inventarizácia aktív, analýza rizík, námety na bezpečnostné opatrenia a lepšie spĺňanie zákonov 69/2018 Z.z., 95/2019 Z.z, vyhlášky NBÚ č. 362/2018 Z.z a vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z.z.

Ako KPI projektu (P0193 - Počet nasadených nástrojov na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov) bude nasadený SW nástroj na monitorovanie a riadenie bezpečnostných incidentov.

Miestom realizácie je sídlo našej organizácie.

V rámci projektu sú realizované nasledovné aktivity, ktorých popis je v ďalších kapitolách:

- Analýza a Dizajn
- Implementácia
- Testovanie
- Nasadenie

3. Implementácia projektu

3.1. Aktivity projektu

Aktivita **Analýza a dizajn** bude pozostávať z nasledovných častí:

- analýza aktuálneho stavu a súladu s legislatívnymi požiadavkami,
- inventarizácia a klasifikácia informačných aktív a kategorizácia IS a sietí,
- analýza rizík a analýza dopadov,
- zavedenie procesu riadenia rizík a procesu governance IB a KyB,
- dodávka produktov definovaných v tab. nižšie na základe šablón MIRRI,
- analýza zavedenia klientskeho nástroja (modulu) evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík a incidentov.

Aktivita **Nasadenie** pozostáva z nasadenia offline klientskeho nástroja evidencie informačných aktív, rizík a incidentov.

3.2. Produkty, ktoré projekt dodáva

Minimálny rozsah požiadaviek zadávateľa zákazky je:

ID	Aktivita/prevádzková dokumentácia (výstup)	Poznámka
1.1	Posúdenie súladu s bezpečnostnými požiadavkami zákonom č. 69/2018 Z.z. (vyhlášky NBÚ č. 362/2018 Z. z.) ako aj 95/2019 (vyhlášky 179/2020 Z.z.) a návrh strategického akčného plánu úloh na zabezpečenie súladu	Výsledkom posúdenia súladu bude rozdielová analýza, ktorá musí obsahovať minimálne tieto kapitoly: • organizácia kybernetickej bezpečnosti, • riadenie aktív, hrozieb a rizík, • personálna bezpečnosť, • riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov, • technické zraniteľností systémov a zariadení, • riadenie bezpečnosti sietí a informačných systémov, • riadenie prevádzky, • riadenie prístupov, • kryptografické opatrenia, • riešenie kybernetických bezpečnostných incidentov, • monitorovanie, testovanie bezpečnosti a bezpečnostné audity, • fyzická bezpečnosť a bezpečnosť prostredia, • riadenie kontinuity procesov. Výstupom rozdielovej analýzy bude zoznam rozdielových zistení, stanovujúcich, do akej miery sú súčasné bezpečnostné opatrenia objednávateľa v zhode s požiadavkami platnej legislatívy. Strategický akčný plán úloh bude obsahovať opatrenia (organizačné, procesné, technické), ktoré je potrebné prijať, aby boli naplnené požiadavky platnej legislatívy, vrátane harmonogramu pre prijatie týchto opatrení.
1.2	Vypracovanie interných smerníc a prevádzkovej dokumentácie riadenia IB a KyB:	Smernice budú pokrývať nasledujúce oblasti: • bezpečnostná stratégia kybernetickej bezpečnosti, • klasifikácia informácií a kategorizácia sietí a informačných systémov, • organizácia kybernetickej bezpečnosti, • riadenie aktív, hrozieb a rizík, • personálna bezpečnosť, • riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov, • technické zraniteľností systémov a zariadení, • riadenie bezpečnosti sietí a informačných systémov, • riadenie prevádzky siete a informačného systému, • riadenie prístupov, • kryptografické opatrenia, • riešenie kybernetických bezpečnostných incidentov,

ID	Aktivita/prevádzková dokumentácia (výstup)	Poznámka
		• monitorovanie, testovanie bezpečnosti a bezpečnostné audity, • fyzická bezpečnosť a bezpečnosť prostredia, • riadenie kontinuity procesov, • bezpečnostný projekt, • koncepcia rozvoja. Výstupom aktivity bude interná dokumentácia a smernice uvedené nižšie.
1.2.1	Stratégia kybernetickej bezpečnosti	V štruktúre a v súlade s obsahovými požiadavkami podľa prílohy č. 1 vyhlášky 362
1.2.2	Bezpečnostná politika	V štruktúre a v súlade s obsahovými požiadavkami podľa prílohy č. 1 vyhlášky 362
1.2.3	Smernica pre riadenie informačnej bezpečnosti	
1.2.4	Klasifikácia informácií a kategorizácia sietí a informačných systémov	Súčasťou je aj transfer know how, aby si bola organizácia schopná klasifikáciu následne realizovať aj vlastnými silami.
1.2.5	Smernica výkonu analýzy rizík a analýzy dopadov (AR/BIA)	
1.2.6	Smernica o bezpečnej prevádzke IS a sietí	Bude pokrývať najmä oblasti: • bezpečná správa a prevádzka IS a sietí, • riadenie zmien, • riadenie kapacít, • riadenie záplat a aktualizácii, • zálohovanie dát, • posudzovanie technických zraniteľnosti, • - bezp. požiadavky pre prístupové práva a účty privilegovaných používateľov.
1.2.7	Smernica o monitorovaní a riešení kybernetických bezpečnostných incidentov	
1.2.8	Politika BCM vrátane stratégie obnovy a návrh pred-vyplnenej šablóny pre BCP a DRP	
1.2.9	Smernica pre bezpečný vývoj a údržbu aplikácií a IS (Secure Software Development Life Cycle – SSDLC) a návrh bezpečnostných požiadaviek pre aplikácie podľa klasifikačných stupňov	Bude pokrývať všetky fázy SSDLC z pohľadu bezpečnosti a bezpečnostných požiadaviek.
1.2.10	Bezpečnostný projekt informačných systémov	Bezpečnostný projekt informačných systémov podľa 95/2019 Z.z. pre informačné systémy kategórie 3 v zmysle 69/2018 Z.z.
1.3	Inventarizácia, klasifikácia a kategorizácia	Výstupom aktivity bude realizácia inventarizácie a klasifikácie informačných aktív (vytvorenie zoznamu aktív a ich klasifikácie z pohľadu dôvernosti, integrity a dostupnosti) a kategorizácie IS a sietí na základe klasifikácie.

ID	Aktivita/prevádzková dokumentácia (výstup)	Poznámka
		Súčasťou je aj transfer know how, aby si bola organizácia schopná klasifikáciu a kategorizáciu následne realizovať aj vlastnými silami.
1.4	Vykonanie analýzy rizík a analýzy dopadov	Analýza bude zahŕňať: • identifikáciu rizík vplývajúcich na aktíva, ich ohodnotenie a ich možné dopady, • zmapovanie a ohodnotenie existujúcich bezpečnostných opatrení na elimináciu rizík, • návrh bezpečnostných opatrení (organizačné, procesné, technické) na elimináciu rizík. • Výstupom bude katalóg rizík s navrhnutým spôsobom riadenia jednotlivých rizík. Výstupom bude vykonaná AR/BIA podľa jednotnej smernice (metodiky) pre dátovo-procesné aktíva (biznis agendy) a IKT zdroje, ktoré tieto agendy podporujú. Súčasťou je aj transfer know how, aby si bola organizácia schopná tieto analýzy opakovane realizovať aj vlastnými silami.
1.5	Návrh katalógu rizík a spôsobov ich riadenia	Návrh katalógu rizík a spôsobu ich udržiavania, aktualizácie a riadenia (mitigácie), ktorý bude obsahovať identifikované riziká z AR/BIA a spôsoby (možnosti) ich riadenia (mitigácie), vrátane zavedenia formalizovaného a opakovaného procesu riadenia rizík.
1.6	Žiadosť o audit Kybernetickej bezpečnosti podľa zákona č. 69/2018 Z.z.	Vypracovanie návrhu žiadosti o audit Kybernetickej bezpečnosti
1.7	Implementácia klientského modulu evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík a incidentov	Implementácia klientskeho modulu poskytnutého MIRRI z projektu CMRKB pre evidenciu informačných aktív, ich klasifikácie, kategorizácie IS a sietí a riadenie identifikovaných rizík a incidentov.

Konkrétnemu naplneniu KPI (P0193 - Počet nasadených nástrojov na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov) prispieva nasadenie produktu z bodu 1.7, ktorý predstavuje nástroj na monitorovanie a riadenie bezpečnostných incidentov.

V prípade technologických opatrení verejný obstarávateľ požaduje konkrétny technologický návrh na základe technickej špecifikácie a parametrov informačnej siete verejného obstarávateľa. Uchádzač vytvorí dokument s presným technickým popisom riešenia a špecifikáciami hardvéru resp. softvéru.

Vyššie je uvedený minimálny rozsah požiadaviek na produkty, ktoré projekt dodáva. Uchádzač má možnosť rozšíriť spektrum ponúknutých a v prípade úspechu uchádzača aj dodanie produktov nad rámec týchto minimálnych požiadaviek. Produktom nad rámec minimálnych požiadaviek sa rozumie dokument alebo software, ktorý tematicky rozširuje dodávané produkty na základe skúsenosti dodávateľa z historicky realizovaných projektov obdobného charakteru,

tak by obstarávateľ dosiahol ďalšie kroky potrebné k realizácii auditu kybernetickej bezpečnosti. Cieľom je aby obstarávateľ dostal produkt so zvýšenou hodnotou za ekonomicky najlepších podmienok.

3.3. Formy spolupráce a súčinnosti

- Verejný obstarávateľ požaduje, aby realizáciu predmetu zákazky úspešný uchádzač zabezpečoval prostredníctvom osôb, ktoré sú technicky a odborne spôsobilé na jeho realizáciu.
- Verejný obstarávateľ požaduje aby úspešný uchádzač vykonal fyzickú obhliadku priestorov a konkrétnych zariadení výpočtovej techniky obstarávateľa za účelom zistenia skutkového stavu a určenia potencionálnych fyzicko-objektových rizík.
- Verejný obstarávateľ požaduje aby úspešný uchádzač zabezpečil fyzickú prítomnosť zástupcu počas auditu kybernetickej bezpečnosti, ktorý poskytne podporu obstarávateľovi počas auditu.

3.4. Záruka a záručná doba

Všetky skutočnosti, ktoré budú počas auditu kybernetickej bezpečnosti vyhodnotené ako nezhody a neboli identifikované vykonaním rozdielovej analýzy sú predmetom záruky a úspešný uchádzač je povinný navrhnúť opatrenia na ich odstránenie.

Záručná doba končí úspešným auditom kybernetickej bezpečnosti, alebo neúspešným auditom, ak všetky nezhody zistené počas auditu boli identifikované v rozdielovej analýze. Verejný obstarávateľ vykoná audit kybernetickej bezpečnosti do 6 mesiacov od ukončenia zákazky. Ak audit v tejto dobe nebude vykonaný, záručné doba bude ukončená.

3.5. Špecifikácia používaných riešení

Riešenie	**Stav**
Počet desktopov	60
Počet notebookov	220
Počet serverov (fyzické, virtuálne)	20/150
Active Directory	Áno
File Server	Áno
Spôsob zálohovania dát	Dátová knižnica, Pásková knižnica
Zabezpečenie perimetra (firewall)	Cisco
Zabezpečenie pracovný staníc (antivírus)	Antivírus, Bitlocker
Zabezpečenie privilegovaných účtov	Áno
Manažovanie technických zraniteľností zariadení podľa výrobcov	Áno
Mailový server spravovaný u seba alebo je hostovaný	On-premise /Cloud
Webové sídlo spravované u seba alebo je hostované	On-premise
IT technické zabezpečenie: technici priamo ako zamestnanci alebo sa jedná o externého dodávateľa	Externí dodávatelia/Interní technici
Vzdialené prístupy (VPN)	Áno Cisco Any Connect

Mobilné prístupy	Áno Cisco Any Connect
Dvojfaktorovú autentifikácia	Áno - správcovia (plánujeme nasadiť v 2021
Smernice/interné riadiace dokumenty v oblasti informačnej bezpečnosti	Áno
Implementované systémy monitoringu siete, aplikácií, zbieranie logov	Flowmon, Proxy, F5
Všetky operačné systémy, biosy a firmvér aktualizované na najnovšiu verziu	N/A
Systémy, aplikácie a zariadenia ktoré sú v súčasnosti nepodporované výrobcom	N/A

HARMONOGRAM

Trvanie Etapy	**Obsah etapy - činnosti**	**Termín realizácie (počet prac. dní)**
Začiatok projektu	Začiatok projektu	T1 = T0 + 5
Fáza 1 cca 6 mesiacov	Analýza a dizajn (predpokladaný rozsah v zmysle projektu - 85 človekodní) Etapa zahŕňa odovzdanie produktov (výstupov) 1.1. – 1.6. v zmysle opisu predmetu zákazky, bod 3.2	T2 = T1 + 124
Fáza 2 cca 3 mesiace	Nasadenie (predpokladaný rozsah v zmysle projektu - 13 človekodní) Etapa zahŕňa poskytovanie služieb podľa bodu 1.7. v zmysle opisu predmetu zákazky, bod 3.2	T3 = T2 + 62

T0 – dátum vstupu do platnosti zmluvy o dielo.

Dni použité pre výpočet termínov sú pracovné dni.

V prípade, že bude možné realizovať plnenie jednotlivých etáp v skorších termínoch, na ktorých sa Zmluvné strany dohodnú, nebude potrebné takto upravené termíny predložiť na schválenie.

Trvanie Etapy	Obsah etapy - činnosti	Termín realizácie (počet prac. dní)
Začiatok projektu	Začiatok projektu	T1 = T0 + 5
Fáza 1 cca 6 mesiacov	Analýza a dizajn (predpokladaný rozsah v zmysle projektu - 85 človekodní) Etapa zahŕňa odovzdanie produktov (výstupov) 1.1. – 1.6. v zmysle opisu predmetu zákazky, bod 3.2	T2 = T1 + 124
Fáza 2 cca 3 mesiace	Nasadenie (predpokladaný rozsah v zmysle projektu - 13 človekodní) Etapa zahŕňa poskytovanie služieb podľa bodu 1.7. v zmysle opisu predmetu zákazky, bod 3.2	T3 = T2 + 62

T0 – dátum vstupu do platnosti zmluvy o dielo.

Dni použité pre výpočet termínov sú pracovné dni.

V prípade, že bude možné realizovať plnenie jednotlivých etáp v skorších termínoch, na ktorých sa Zmluvné strany dohodnú, nebude potrebné takto upravené termíny predložiť na schválenie.

Príloha č. 3

Zoznam zúčastnených expertov na projekte s názvom **„Príprava na bezpečnostný audit Prešovského samosprávneho kraja"** :

1) Ing. Jozef Stanko
2) Ing. Pavol Rybár

.....

A4 Technology, s. r. o.
v.r. Ing. Július Činčala, LL.M
konateľ