**Vytvorenie vrcholovej dokumentácie riadenia informačnej a kybernetickej bezpečnosti pre ISVS Národného centra zdravotníckych informácií**

Predmetom zákazky je vytvorenie vrcholovej dokumentácie riadenia informačnej a kybernetickej bezpečnosti pre ISVS Národného centra zdravotníckych informácií (ďalej len „NCZI“), ktoré boli zaradené medzi základné služby podľa § 3, písm. k), bodu 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej iba „ZoKIB“). Bezpečnostná dokumentácia musí byť vypracovaná v súlade s požiadavkami ZoKIB a nadväzujúcej vyhlášky č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej iba „Vyhláška o BO“). Neoddeliteľnou súčasťou predmetu dodávky musí byť návrh vrcholovej a riadiacej dokumentácie s požiadavkami zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej iba „Zákon o ITVS“) a na neho nadväzujúcim vykonávajúcim predpisom Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy vrátane návrhu bezpečnostných politík. Vypracovanie dokumentácie v oblasti informačnej a kybernetickej bezpečnosti musí taktiež reflektovať na požiadavky Vyhlášky č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy. Súčasťou bude analýza a zapracovanie požiadaviek vyhlášky č. 85/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o riadení projektov a zapracovanie požiadaviek pripravovanej vyhlášky č. 149/2021 Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky o spôsoboch a postupoch pri elektronizácii agendy verejnej správy do riadiacej dokumentácie.

V súlade s ustanoveniami § 14 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov musí predmet dodávky obsahovať návrh úpravy a spôsobu aplikovania procesov, nastavenia riadenia bezpečnosti a politík pre NCZI, a to najmä v týchto oblastiach:

1. Personálna bezpečnosť
2. Fyzická bezpečnosť a bezpečnosť prostredí s osobitným režimom
3. Riadenie informačnej bezpečnosti
4. Kontrolné mechanizmy informačnej bezpečnosti
5. Správa a monitorovanie bezpečnostných incidentov
6. Ochrana proti nežiaducemu a škodlivému kódu
7. Sieťová bezpečnosť
8. Aktualizácia softvéru, manažment zraniteľností a opráv
9. Zálohovanie a zabezpečenie nepretržitosti a obnovy
10. Riadenie prístupu
11. Aktualizácia informačno-komunikačných technológií
12. Účasť tretej strany
13. Legislatívna bezpečnosť
14. Kryptografia a možnosti jej nasadenia

 Verejný obstarávateľ preto požaduje od víťazného uchádzača úpravu existujúcej a/alebo vypracovanie novej dokumentácie v nasledovnom rozsahu:

**Etapa 1: Vypracovanie bezpečnostnej dokumentácie podľa ZoKIB**

Bezpečnostná dokumentácia musí byť vypracovaná alebo aktualizovaná s ohľadom na prevádzkovanú infraštruktúru IKT, aplikačnú a bezpečnostnú architektúru a implementované bezpečnostné opatrenia, organizačné usporiadanie, pracovné roly, zodpovednosti a rozdelenie právomocí, zaužívaný rámec riadenia operačných rizík, organizačnú kultúru a spoločenskú zodpovednosť NCZI. Dokumentácia musí určiť všetky relevantné požiadavky, mapovať ich plnenie v prostredí NCZI a stanoviť pravidlá priebežnej kontroly ich dodržiavania.

Bezpečnostná dokumentácia musí obsahovať:

1. bezpečnostnú stratégiu kybernetickej bezpečnosti a informačnej bezpečnosti v súlade s požiadavkami na jej štruktúru a obsah uvedenými v Prílohe č. 1 Vyhlášky o BO
2. klasifikáciu informácií a kategorizáciu sietí a informačných systémov,

Klasifikácia informácií a kategorizácia sietí a informačných systémov sa vykoná v klasifikačnej schéme v súlade so štruktúrou klasifikácie informácií a kategorizácie sietí a informačných systémov podľa prílohy č. 2 Vyhlášky o BO. Obstarávateľ disponuje vlastnou klasifikáciou informácií a kategorizáciou sietí a informačných systémov a požaduje vykonať mapovanie na klasifikáciu v klasifikačnej schéme v súlade so štruktúrou klasifikácie informácií a kategorizácie sietí a informačných systémov podľa prílohy č. 2 Vyhlášky o BO.

**Etapa 2: Vypracovanie bezpečnostnej dokumentácie v súlade so zákonom o ITVS.**

**Vrcholová a riadiaca dokumentácia musí obsahovať najmä:**

1. Opatrenia v oblasti informačných technológií verejnej správy pokrývajú konkrétne:
* Vzory bezpečnostnej dokumentácie pre oblasť riadenia kontinuity činností (analýza dopadov, plány kontinuity činností, plány obnovy činností IT a plány testov a ich záznamy).
* Vnútorný predpis pre systém riadenia informačných technológií verejnej správy.
* Návrh nastavenia organizačnej štruktúry, procesov a nástrojov potrebných na riadenie v súlade s požiadavkami definovanými v § 14, ods. 5 zákona o ITVS.
* Vnútorný predpis na zabezpečenie riadenia kľúčových zdrojov.
* Vnútorný predpis pre nastavenie riadenia zmluvných vzťahov pre poskytovanie služieb v súlade s požiadavkami definovanými v § 14, ods. 6 zákona o ITVS.
* Vnútorný predpis pre riadenie kvality
* Vnútorný predpis pre riadenie rizík
* Systém riadenia pre oblasť obstarávania a implementácie informačných technológií verejnej správy v súlade s požiadavkami definovanými v § 15 zákona o ITVS.
* Vnútorný predpis riadenia pre oblasť prevádzky, servisu a podpory informačných technológií verejnej správy v súlade s požiadavkami definovanými v § 16 zákona o ITVS.
* Vnútorný predpis definujúci systém riadenia pre oblasť monitorovania a hodnotenia informačných technológií verejnej správy v súlade s požiadavkami definovanými v § 17 zákona o ITVS.
* Vnútorný predpis popisujúci oblasť riadenia bezpečnosti v oblasti plánovania a organizácie v súlade s požiadavkami definovanými v § 19 zákona o ITVS.
* Vnútorný predpis popisujúci systém riadenia bezpečnosti informačných technológií verejnej správy pre oblasť obstarávania a implementácie v súlade s požiadavkami definovanými v § 20 zákona o ITVS.
* Vnútorný predpis definujúci systému riadenia bezpečnosti informačných technológií verejnej správy v oblasti prevádzky, servisu a podpory v súlade s požiadavkami definovanými v § 21 zákona o ITVS.
* Vnútorný predpis popisujúci systém riadenia bezpečnosti informačných technológií verejnej správy v oblasti monitoringu a hodnotenia v súlade s požiadavkami definovanými v § 22 zákona o ITVS.
1. Návrh bezpečnostných politík

Na základe bezpečnostnej stratégie kybernetickej bezpečnosti pripraví dodávateľ návrh bezpečnostných politík pokrývajúci nasledujúce oblasti:

* Bezpečnostná politika pre oblasť organizácie informačnej bezpečnosti v súlade s požiadavkami definovanými v § 5 Vyhlášky o BO.
* Bezpečnostná politika pre oblasť riadenia aktív, hrozieb a rizík bezpečnosti v súlade s požiadavkami definovanými v § 6 Vyhlášky o BO.
* Bezpečnostná politika pre oblasť personálnej bezpečnosti v súlade s požiadavkami definovanými v § 7 Vyhlášky o BO.
* Bezpečnostná politika pre oblasť riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov v súlade s požiadavkami definovanými v § 8 Vyhlášky o BO.
* Bezpečnostná politika pre oblasť technických zraniteľností systémov a zariadení v súlade s požiadavkami definovanými v § 9 Vyhlášky o BO.
* Bezpečnostná politika pre oblasť riadenia bezpečnosti sietí a informačných systémov v súlade s požiadavkami definovanými v § 10 Vyhlášky o BO.
* Bezpečnostná politika pre oblasť riadenia bezpečnosti prevádzky siete a informačného systému v súlade s požiadavkami definovanými v § 11 Vyhlášky o BO.
* Bezpečnostná politika pre oblasť riadenia prístupov v súlade s požiadavkami definovanými v § 12 Vyhlášky o BO.
* Bezpečnostná politika pre oblasť kryptografických opatrení v súlade s požiadavkami definovanými v § 13 Vyhlášky o BO.
* Bezpečnostná politika pre oblasť riešenia kybernetických bezpečnostných incidentov v súlade s požiadavkami definovanými v § 14 Vyhlášky o BO, vrátane Plánu zvládania incidentov (IMP).
* Bezpečnostná politika pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov v súlade s požiadavkami definovanými v § 15 Vyhlášky o BO.
* Bezpečnostná politika pre oblasť fyzickej bezpečnosti a bezpečnosti prostredia v súlade s požiadavkami definovanými v § 16 Vyhlášky o BO.
* Bezpečnostná politika pre oblasť riadenia kontinuity procesov v súlade s požiadavkami definovanými v § 17 Vyhlášky o BO.

, ktoré budú verejným obstarávateľom obsahovo integrované do:

* Smernice, ktorou sa definujú pravidlá klasifikácie informácií, ich inventarizácie a manipulácie s nimi.
* Metodického usmernenia k vypracovaniu analýzy rizík informačnej bezpečnosti.
* Smernice na riadenie kontinuity činností v NCZI.
* Smernice o pravidlách práce v počítačovej sieti NCZI.
* Smernice, ktorou sa definujú pravidlá pre hlásenie a riešenie bezpečnostných incidentov.
* Smernice, ktorou sa definujú pravidlá na manažment rizík informačnej bezpečnosti.
* Smernice na zabezpečenie správy a prevádzky informačných systémov NCZI.
* Smernice o riadení prístupových práv používateľov do informačných systémov NCZI.
* Politiky kybernetickej bezpečnosti a informačnej bezpečnosti.
* Smernice o postupoch a podmienkach pri presune alebo implementácii informačných systémov do Dátového centra NCZI, ich prevádzke v Dátovom centre NCZI a zavádzaní nových informačných systémov v podmienkach NCZI.
* Smernice, ktorou sa vydáva Bezpečnostný projekt.
* Smernice o centrálnom riadení projektov a žiadostí na vývoj, rozvoj a zrušenie informačných systémov NCZI.

**Etapa 3: Vypracovanie vzoru bezpečnostného projektu podľa zákona ITVS**

Verejný obstarávateľ stanovuje nasledovné minimálne požiadavky na bezpečnostný projekt a súvisiacu pracovnú dokumentáciu:

* bezpečnostný projekt ISVS podľa § 23 ods. 1 a 2 zákona o ITVS,
* návrh osobitných opatrení na úseku bezpečnosti v súlade s požiadavkami definovanými v § 23, ods. 3 až 5 zákona o ITVS,
* pracovná bezpečnostná dokumentácia kybernetickej bezpečnosti, ktorá zahŕňa bezpečnostné návody, na zálohovanie a archiváciu, riadenie testovania, riadenie interných auditov, riadenie profylaktických činností a riadenie konfigurácií, ktoré predstavujú súhrn predpísaných krokov na vykonanie bezpečnostných politík a bezpečnostných štandardov prostredníctvom konkrétnych akcií.

Nasledovné dokumenty predloží uchádzač verejnému obstarávateľovi až v predmetnom obstarávaní (nie v prieskume trhu)– verejný obstarávateľ túto informáciu uvádza z dôvodu správneho výpočtu predpokladanej hodnoty zákazky.

* platný certifikát systému manažérstva bezpečnosti informácií podľa EN ISO 27001
* platný certifikát systému manažérstva kvality podľa EN ISO 9001
* platného certifikátu systému manažérstva služieb IT podľa EN ISO 20000 v oblasti vývoja, riadenia, poskytovania podpory servisu a outsourcingu IT služieb
* profesijné životopisy príslušných expertov, predloží doklady, dokumenty alebo údaje (napr. vlastnoručne podpísaný profesijný životopis, doklad o najvyššom dosiahnutom vzdelaní, certifikát alebo osvedčenie) a zoznam praktických skúseností experta, ktorý bude zodpovedný za plnenie zmluvy na poskytnutie služieb; predkladané doklady, dokumenty a údaje musia obsahovať súhlas dotknutej osoby so správou, spracovaním a uchovaním osobných údajov v zmysle zákona č. 18/2018 Z. z. ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

**Expert pre bezpečnosť informácií:**

1. minimálne 3-ročná preukázateľná odborná prax v oblasti bezpečnosti informačných technológií,
2. minimálne dve (2) preukázateľné profesionálne praktické skúsenosti v oblasti riadenia bezpečnosti pri vývoji a nasadení IKT systému, pričom minimálne jedna (1) praktická skúsenosť s implementáciou systému riadenia informačnej bezpečnosti v súlade s normou STN ISO/IEC 27001;
3. platný certifikát profesionála riadenia informačnej bezpečnosti CISSP vydaný neziskovým združením (ISC)2 alebo ekvivalent daného certifikátu od inej akreditovanej autority.

**Expert pre riadenie kontinuity činností:**

1. minimálne 3-ročná preukázateľná odborná prax v oblasti práce s riadením kontinuity činností,
2. minimálne dve (2) preukázateľné profesionálne praktické skúsenosti v oblasti riadenia kontinuity činností, plánovania a riadenia kontinuity činností v pozícii kľúčového odborníka pre riadenie kontinuity činností,
3. platný certifikát Business Continuity Institute pre riadenie kontinuity činností alebo ekvivalentný, vydaný vedúcou akreditačnou a certifikačnou autoritou uznávanou medzinárodne v oblasti riadenia kontinuity činností.

**Expert pre riadenie bezpečnosti informačných aktív:**

1. minimálne 3-ročná preukázateľná odborná prax v oblasti riadenia bezpečnosti informačných aktív,
2. minimálne dve (2) preukázateľné profesionálne praktické skúsenosti v oblasti riadenia bezpečnosti informačných aktív;
3. platný certifikát manažérstva informačnej bezpečnosti CISM (resp.CISA) vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou.

Termín trvania zmluvy – dodanie finálnej dokumentácie cca 3 mesiace odo dňa účinnosti zmluvy.

Kritérium hodnotenia: cena celkom za predmet zákazky v eur vrátane DPH

|  |  |
| --- | --- |
| **Názov podpornej služby**  | **Cena v € bez DPH za etapu** |
| **Etapa 1: Vypracovanie bezpečnostnej dokumentácie podľa ZoKIB** |  |
| **Etapa 2: Vypracovanie bezpečnostnej dokumentácie v súlade so zákonom o ITVS.**  |  |
| **Etapa 3: Vypracovanie vzoru bezpečnostného projektu podľa zákona ITVS** |  |
|  |  |
| **Cena spolu bez DPH** |
| **DPH** |
| **Cena celkom vrátane DPH** |