B.1 OPIS PREDMETU ZÁKAZKY

Predmetom zákazky je vytvorenie vrcholovej dokumentácie riadenia informačnej a kybernetickej bezpečnosti pre IS Národného centra zdravotníckych informácií (ďalej len „NCZI“), ktoré boli zaradené medzi základné služby podľa § 3, písm. l), bodu 1 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej iba „ZoKIB“). Informácie o základných službách v zmysle ZoKIB sú uvedené v Zozname základných služieb vedených NBÚ SR na www.nbu.gov.sk. 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 vyhlášky č. 547/2021 Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky o elektronizácii agendy verejnej správy. Verejný obstarávateľ požaduje primerane aplikovať ustanovenia vyhlášky č. 85/2020 Z. z. o riadení projektov.

Verejný obstarávateľ všeobecne potrebuje nastaviť procesy, aby boli v súlade s legislatívnymi požiadavkami. Preto požaduje 1 a 2 úroveň dokumentácie, smernice a riadiacu dokumentáciu. Nie je zámerom technické nastavenia, alebo technická dokumentáciu v rámci jednotlivých IS.

V súlade s ustanoveniami § 20 ZoKIB a § 14 a § 22 zákona o ITVS musí predmet dodávky obsahovať návrh úpravy a spôsobu aplikovania procesov, nastavenia riadenia bezpečnosti a politík pre NCZI, a to najmä v týchto oblastiach:

1. organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
2. riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
3. personálnej bezpečnosti,
4. riadenia prístupov,
5. riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
6. bezpečnosti pri prevádzke informačných systémov a sietí,
7. hodnotenia zraniteľností a bezpečnostných aktualizácií,

8. ochrany proti škodlivému kódu,
9. sieťovej a komunikačnej bezpečnosti,
10. akvizície, vývoja a údržby informačných sietí a informačných systémov,
11. zaznamenávania udalostí a monitorovania,
12. fyzickej bezpečnosti a bezpečnosti prostredia,
13. riešenia kybernetických bezpečnostných incidentov,
14. kryptografických opatrení,
15. kontinuity prevádzky,
16. zálohovania a zabezpečenie nepretržitosti a obnovy,
17. auditu, riadenia súladu a kontrolných činností,
18. kontrolných mechanizmov informačnej bezpečnosti,
19. správy a monitorovania bezpečnostných incidentov,
20. aktualizácie softvéru, manažmentu zraniteľností a opráv.

Verejný obstarávateľ deklaruje, že existujúca dokumentácia bola vypracovaná v súlade so zákonom č.275/2006 o informačných systémoch verejnej správy a má viac ako 300 strán. 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:

a) bezpečnostnú stratégiu kybernetickej bezpečnosti a informačnej bezpečnosti v súlade s požiadavkami na jej štruktúru a obsah uvedenými v Prílohe č. 1 Vyhlášky o BO
b) klasifikáciu informácií a kategorizáciu sietí a informačných systémov podľa prílohy č. 2 Vyhlášky o BO. Dotknuté IS sú vládny cloud, verejný cloud, privátny cloud DC a interná sieť.
c) vypracovanie bezpečnostných politík podľa časti B Prílohy č. 1 vyhlášky č. 362/2018 Z. z.

Verejný obstarávateľ **nepožaduje** od úspešného uchádzača vypracovanie zoznamu komponentov sietí a informačných systémov poskytujúcich základné služby a ich za kategorizovanie. Požaduje definovať spôsob ich klasifikácie a kategorizácie.
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 nedisponuje 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. Verejný obstarávateľ požaduje vypracovanie bezpečnostnej dokumentácie tak ako je to uvedené v Opise predmetu zákazky.

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

Verejný obstarávateľ požaduje od víťazného uchádzača vypracovanie bezpečnostnej dokumentácie podľa zákona o ITVS. NCZI od víťazného uchádzača požaduje posúdenie smerníc uvedených v tomto zozname a ich prepracovanie. NCZI od víťazného uchádzača požaduje identifikáciu služieb, ktoré vykonáva a poskytuje na účely poskytovania služieb verejnej správy, služieb vo verejnom záujme a verejných služieb (ďalej len „príslušné služby“). NCZI od víťazného uchádzača požaduje identifikovať príslušné služby a zadefinovať parametre potrebnej úrovne poskytovania týchto služieb.

Požadovaná miera detailu vypracovania dokumentácie je definovaná úrovňou špecifikácie konkrétnych detailov súvisiacich s príslušnými ustanoveniami § 14 – 22 zákona o ITVS. Požadovaná miera detailnosti zo strany NCZI pre vypracovanie príslušných politík je definovaná v rozsahu ustanovení § 3 – 17 vyhlášky o BO. Pri tvorbe príslušných bezpečnostných politík je postačujúce rámcovo zohľadniť príslušné požiadavky v §3 – 17 vyhlášky o BO a štruktúra BP bude kopírovať rozsah definovaný prílohou č. 1 časť B vyhlášky o BO.

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.

2. 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:

- jeden 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. 1 a 2 zákona o ITVS, v detaile podľa 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 na úrovni požadovaných zodpovednosti, rolí, procesov, pravidiel. Nie detailne vypracovanie, ale procesne.