Príloha č. 3 Špecifikácia predmetu zákazky

1. **Predmet zákazky**
   a) **všeobecná špecifikácia predmetu zákazky**
   Predmetom zákazky je:
   - Podpora zavedenia a dosiahnutie súladu podmienok prevádzkovania kompletného informačného systému verejného obstarávateľa so ZoKB pre nasledovné základné služby:

Základná služba
isvs_8641 Register podaných prihlášok na verejné zdravotné poistenie
isvs_8635 Register poskytovateľov zdravotnej starostlivosti
isvs_8634 Register zdravotníckych pracovníkov
isvs_8631 Centrálny register poistencov
isvs_8630 Evidencia a Správa Formulárov
isvs_8629 Register úmrtí fyzických osôb alebo vyhlásení za mŕtveho
isvs_8628 Evidencia pitiev

- Vykonanie posúdenia poskytovanej základnej služby aj pre ďalšie informačné systémy verejnej správy verejného obstarávateľa zverejnené na META IS v zmysle požiadaviek § 2 ods. 2 vyhlášky NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška č. 362/2018 Z. z.“) s cieľom vymedziť základnú službu a s ňou súvisiacu infraštruktúru, architektúru a organizáciu a riadenie.
- Vypracovanie dokumentu alebo dokumentov „Metodika riadenia aktív, hrozieb a rizík“ v súlade s požiadavkami § 6 ods. 3 vyhlášky č. 362/2018 Z. z. a v súlade s „dobrou praxou“ (napr. normou ISO/IEC 27005).
- Vykonanie analýzy rizík v rozsahu určenom ZoKB. Výstupom bude dokument, ktorý musí minimálne obsahovať návrhy organizačných a technických bezpečnostných opatrení na elimináciu detegovaných rizík. Analýzou budú identifikované najmä hrozby, aktíva a ich zraniteľnosti, vlastníci aktív.
- Vykonanie rozdielovej analýzy bezpečnostných opatrení oproti stavu požadovanému ZoKB a vyhláškou č. 362/2018 Z. z.
- V rámci rozdielovej analýzy bezpečnostných opatrení oproti stavu požadovanému ZoKB a vyhláškou č. 362/2018 Z. z. požaduje verejný obstarávateľ aj detailné preverenie miery schopnosti odolávať kybernetickým útokom.
- Zaškolenie určených zamestnancov verejného obstarávateľa na vykonávanie procesu „Riadenie aktív, hrozieb a rizík“ v súlade s dokumentom „Metodika riadenia aktív, hrozieb a rizík“.
- Vypracovanie dokumentu „Bezpečnostná stratégia kybernetickej bezpečnosti v súlade s § 3 vyhláškou č. 362/2018 Z. z. a štruktúrou, ktorú definuje príloha č.1 vyhlášky č.362/2018 Z. z.
- Vypracovanie dokumentov „Metodika pre klasifikáciu informácii a kategorizáciu IKT komponentov“ a „Metodika evidencie komponentov“, pričom je možné metodiky zlúčiť do jedného dokumentu. Je potrebné navrhnúť a popísať formy evidencie (komponentov, informácií) tak, aby metodika mohla byť používaná univerzálne. Cieľom je plnenie požiadaviek, ktoré definuje § 4 vyhláška č.362/2018 Z. z.
- V dokumente „Metodika evidencie komponentov“ popísať mapovanie „aktívum vs. komponent/komponenty“ resp. popísať súvis/väzby medzi riadením aktív a evidenciou komponentov.
- Vykonanie klasifikácie informácií (vrátane ich prvotného detegovania), vytvorenie zoznamu komponentov (pre informačné systémy a siete verejného obstarávateľa) a kategorizácia všetkých

komponentov do príslušných bezpečnostných kategórii v súlade s prílohou č. 2 vyhlášky č. 362/2018 Z. z.

- Vypracovanie dokumentu „Požiadavky na bezpečnostné opatrenia“, ktorý stanoví konkrétne minimálne bezpečnostné opatrenia pre kategórie sietí a informačných systémov verejného obstarávateľa.
- Zaškolenie určených zamestnancov verejného obstarávateľa na vykonávanie činností potrebných k udržiavaniu „Zoznamu komponentov“ v aktuálnom stave.
- Návrh a vypracovanie potrebných bezpečnostných politík, smerníc a procesov a podpora pri ich zavedení do praxe vyplývajúcich z platnej právnej úpravy.
- Všetky návrhy, odporúčania a dokumentácia musia byť v súlade so zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov a v súlade s vyhláškou č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
- Aktívna spolupráca úspešného uchádzača v celom rozsahu poskytovania poradenských služieb.
- Odporúčanie konkrétneho riešenia (technológie, systémov) pre zabezpečenie súladu so ZoKB a príslušnými zákonmi a vyhláškami. Dodávka technických opatrení nie je predmetom zadania.
- Príprava verejného obstarávateľa na vykonanie auditu kybernetickej bezpečnosti podľa ZoKB (ďalej len „audit kybernetickej bezpečnosti“) a účasť na tomto audite kybernetickej bezpečnosti.
- Poskytnutie služby Manažéra kybernetickej bezpečnosti nie je predmetom zákazky.

Informácia k súčasnému stavu:

Dostupnosť riadiacej dokumentácii (predpisy) stanovujúce pravidlá pre:

a. riadenie bezpečnostnej architektúry - V podobe vrcholového dokumentu
b. riadenie informačnej bezpečnosti - V podobe vrcholového dokumentu
c. riadenie identít a prístupových práv - V podobe internej smernice
d. riadenie prístupov - NIE
e. bezpečnostný monitoring a správu bezpečnostných záznamov – riešené prostredníctvom Outsourcingu – v podobe zmluvných požiadaviek
f. testovanie bezpečnosti systémov - NIE
g. riadenie rizík a metodiku posudzovania rizík - NIE
h. fyzickú bezpečnosť a bezpečnosť prostredia - V podobe vrcholového dokumentu
i. riešenie bezpečnostných incidentov - ÁNO
j. klasifikáciu informácií a kategorizácia sietí - NIE
k. prácu na diaľku a používanie mobilných zariadení - V podobe vrcholového dokumentu
l. riadenie personálnej bezpečnosti - ÁNO
m. pravidlá komunikácie - ÁNO
n. riadenie dodávateľských služieb - NIE
o. akvizíciu informačných systémov - NIE
p. vývoj a testovanie informačných systémov - V podobe vrcholového dokumentu
q. postupy údržby informačných systémov - V podobe internej smernice
r. riadenie technických zraniteľností a manažment záplat - NIE
s. pravidlá prepájania systémov a prenosu elektronických informácií - NIE
t. riadenie bezpečnosti sietí - V podobe vrcholového dokumentu
u. riadenie zmien infraštruktúry a IS - NIE
v. riadenie kapacity systémov a služieb - NIE
w. riadenie kryptografických opatrení - NIE
x. výkon bezpečnostných auditov - V podobe vrcholového dokumentu
y. spracúvanie osobných údajov a klasifikovaných informácií (ostatných citlivých informácií) - ÁNO
z. poskytovanie súčinnosti tretím stranám - NIE
aa. plánovanie kontinuity prevádzkových činností -NIE
bb. metodiku zálohovania a obnovy informácií - V podobe internej smernice

Klasifikácia informácii a kategorizácia sietí a informačných systémov verejného obstarávateľa nie je vykonaná v zmysle ZoKB.

- Požadovaný termín plnenia:

Úspešný uchádzač je povinný navrhnúť riešenia, odporúčania, nastavenia interných procesov, ktorými sa zosúladí aktuálny stav podmienok prevádzkovania kompletného informačného systému verejného obstarávateľa ako aj riadne odovzdať vypracovanú kompletnú dokumentáciu, v súlade s požiadavkami vyplývajúcimi zo ZoKB a príslušnej právnej úpravy upravujúcej kybernetickú bezpečnosť v termíne do 3 kalendárnych mesiacov odo dňa účinnosti zmluvy o poskytovaní poradenských služieb (ďalej len „zmluva“).

- Požadované trvanie zmluvného vzťahu

Na dobu určitú, odo dňa nadobudnutia účinnosti zmluvy na obdobie do ukončenia auditu kybernetickej bezpečnosti, to je do doručenia záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti verejnému obstarávateľovi a v prípade potreby predkladania nápravných opatrení, do dňa ich predloženia na Národný bezpečnostný úrad, okrem ustanovení nestrácajúcich platnosť a účinnosť aj po ukončení zmluvy.