Opis predmetu zákazky:

„**Informačná a kybernetická bezpečnosť - zavedenie bezpečnostných opatrení a postupov**“

Verejný obstarávateľ pri poskytovaní základných služieb prostredníctvom informačných systémov a zabezpečení prevádzky informačných systémov musí plniť požiadavky legislatívy, vyplývajúce zo:

* zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o KB“),
* zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o ITVS“),
* vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „Vyhláška“).

Uvedené požiadavky predpokladá plniť verejný obstarávateľ najmä implementáciou informačnej bezpečnosti a prijatím bezpečnostných opatrení v rozsahu:

* vypracovanie a aktualizácia riadiacej, prevádzkovej dokumentácie a návrh a realizácia opatrení pre potreby PPA v súlade s legislatívou v oblasti kybernetickej bezpečnosti (tzv. bezpečnostná dokumentácia), ktorá má obsahovať nasledovné:
  + vypracovanie interných smerníc vo vzťahu ku kybernetickej bezpečnosti,
  + klasifikácia informácií a kategorizácia sietí a informačných systémov,
  + bezpečnostná stratégia kybernetickej bezpečnosti,
  + bezpečnostná politika kybernetickej bezpečnosti;
* vykonanie analýzy rizík kybernetickej bezpečnosti a návrh na riadenie rizík,
* plánovanie kontinuity činnosti, vypracovanie návrhu „Stratégie kontinuity a vytvorenie plánov kontinuity“,
* identifikácia parametrov potrebných pre výber budúcich dodávateľov technológie alebo služieb v oblasti informačnej a kybernetickej bezpečnosti – táto služba bude poskytovaná mesačne v rozsahu najviac 2 MD počas doby trvania zmluvy (t. j. najviac 8 MD),
* zaškolenie a podpora pri implementácií navrhnutých riešení informačnej bezpečnosti a udržiavaní súladu s platnou legislatívou v oblasti kybernetickej bezpečnosti.

Jednotlivé oblasti sú bližšie špecifikované nižšie.

1. **Vypracovanie a aktualizácia riadiacej, prevádzkovej dokumentácie a návrh a realizácia opatrení pre potreby PPA v súlade s legislatívou v oblasti kybernetickej bezpečnosti**
2. **Bezpečnostná dokumentácia má obsahovať:**
3. bezpečnostnú stratégiu kybernetickej bezpečnosti,
4. bezpečnostné politiky kybernetickej bezpečnosti,
5. klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
6. návrh - zadokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení; konkrétny obsah môže byť odvodený z princípov niektorého z rámcov riadenia bezpečnostnej architektúry.

Bezpečnostnú dokumentáciu je potrebné vypracovať na základe posúdenia poskytovanej základnej služby, s ktorou súvisí najmä:

1. infraštruktúra informačno-komunikačných technológií,
2. aplikačná architektúra,
3. bezpečnostná architektúra a implementované bezpečnostné opatrenia,
4. organizačné usporiadanie, pracovné role, zodpovednosti a delenie právomocí,
5. zaužívané rámce riadenia operačných rizík,
6. organizačná kultúra a spoločenská zodpovednosť.
7. **Bezpečnostná dokumentácia má obsahovať nasledovné interné smernice vo vzťahu ku kybernetickej bezpečnosti:**
8. smernica na riadenie informačnej bezpečnosti,
9. smernica o monitorovaní a riešení kybernetických bezpečnostných incidentov,
10. smernicu pre používanie IT systémov a služieb,
11. smernicu pre správu a prevádzku IT systémov a služieb,
12. smernicu pre riadenie prístupových práv,
13. smernicu pre klasifikáciu a kategorizáciu informačných aktív,
14. smernicu pre zálohovanie a archiváciu,
15. ďalšie bezpečnostné politiky.
16. **Bezpečnostná stratégia kybernetickej bezpečnosti sa definuje v rozsahu:**
17. bezpečnostných cieľov z hľadiska kybernetickej bezpečnosti, určených aj na základe vykonanej analýzy rizík,
18. spôsobu vyhodnocovania bezpečnostných cieľov, kritérií vyhodnocovania dosahovania bezpečnostných cieľov, spôsobov priebežného hodnotenia ich primeranosti a spôsobov kontroly postupov využívaných na dosahovanie bezpečnostných cieľov,
19. úlohy štatutárneho orgánu prevádzkovateľa základnej služby pri zabezpečovaní kybernetickej bezpečnosti  
    a vyhlásenie o záväzku o podpore kybernetickej bezpečnosti,
20. všeobecných a špecifických zodpovedností a povinností v oblasti kybernetickej bezpečnosti a určenie príslušných bezpečnostných rolí potrebných na riadenie kybernetickej bezpečnosti vrátane určenia rozsahov činností, kompetencií a úloh; rozdelenie rolí na riadiacu zložku, výkonnú zložku a kontrolnú zložku, pričom riadiaca zložka je priamo riadená prevádzkovateľom základnej služby a kontrolná zložka je nezlučiteľná so všetkými ostatnými zložkami,
21. základného rámca na riadenie aktív podľa § 6, od ktorých závisí činnosť sietí a informačných systémov,
22. základného rámca riadenia rizík podľa § 6 v súvislosti s aktívami, od ktorých závisí činnosť sietí a informačných systémov a určenie bezpečnostných opatrení podľa oblastí v zmysle § 20 ods. 3 zákona v závislosti od identifikovaných rizík,
23. rozsahu a periodicity overovania stavu kybernetickej bezpečnosti prostredníctvom auditu kybernetickej bezpečnosti vrátane zhodnotenia súladu bezpečnostnej stratégie a bezpečnostných politík s požiadavkami zákona, iného všeobecne záväzného právneho predpisu, vnútorných predpisov a zmluvnými záväzkami,
24. postupu a zodpovedností pri revízii bezpečnostnej dokumentácie schvaľovanej prevádzkovateľom základnej služby vrátane periodicity pravidelných revízií a jej aktualizácií po každej zmene majúcej na ňu vplyv, ako aj z dôvodov mimoriadnych revízií.
25. **Bezpečnostná politika kybernetickej bezpečnosti (stanovenie základných cieľov a zodpovedností) v rozsahu:**
26. organizácia bezpečnosti:
    * riadenie bezpečnostnej architektúry,
    * systém riadenia kybernetickej bezpečnosti,
    * riadenie identít a prístupových práv,
    * riadenie privilegovaných prístupov,
    * bezpečnostný monitoring a správa,
    * bezpečnostných záznamov;
27. riadenie bezpečnostných rizík:
    * testovanie a bezpečnostná certifikácia systémov,
    * metodika posudzovania vplyvu na ochranu osobných údajov,
    * metodika posudzovania rizík,
    * fyzická bezpečnosť a bezpečnosť prostredia,
    * riešenie bezpečnostných incidentov;
28. riadenie informačných aktív:
    * klasifikácia informácií a kategorizácia sietí,
    * registratúrny poriadok a registratúrny plán,
29. pravidlá správania a dobrej praxe:
    * práca na diaľku a používanie mobilných zariadení,
    * riadenie personálnej bezpečnosti,
    * pravidlá komunikácie;
30. riadenie dodávateľských vzťahov:
    * riadenie dodávateľských služieb,
    * akvizícia informačných systémov;
31. riadenie vývoja a údržby v oblasti informačno-komunikačných technológií:
    * vývoj a testovanie informačných systémov,
    * postupy údržby informačných systémov,
    * riadenie technických zraniteľností a manažment záplat;
32. riadenie a prevádzka informačno-komunikačných technológií:
    * pravidlá prepájania systémov a prenosu,
    * elektronických informácií,
    * riadenie bezpečnosti sietí,
    * riadenie zmien infraštruktúry,
    * riadenie kapacity systémov a služieb,
    * riadenie kryptografických opatrení;
33. riadenie súladu:
    * audit kybernetickej bezpečnosti,
    * spracúvanie osobných údajov a klasifikovaných informácií,
    * poskytovanie súčinnosti tretím stranám;
34. riadenie kontinuity procesov a činností:
    * plány kontinuity prevádzkových činností,
    * plány havarijnej obnovy prevádzky,
    * metodika zálohovania a obnovy informácií.
35. **Bezpečnostné opatrenia sa prijímajú hlavne pre oblasť:**
36. organizácie informačnej bezpečnosti,
37. riadenia aktív, hrozieb a rizík,
38. personálnej bezpečnosti,
39. riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
40. technických zraniteľností systémov a zariadení,
41. riadenia bezpečnosti siete, informačných a komunikačných systémov,
42. riadenia prevádzky,
43. riadenia prístupov,
44. kryptografických opatrení,
45. riešenia kybernetických bezpečnostných incidentov,
46. monitorovania, testovania bezpečnosti a bezpečnostných auditov,
47. fyzickej bezpečnosti a bezpečnosti prostredia,
48. riadenia kontinuity procesov.

Na základe klasifikácie aktív a informačných systémov (klasifikácia podľa prílohy č. 2 Vyhlášky) sa prijímajú bezpečnostné opatrenia podľa prílohy č. 3. Vyhlášky.

Klasifikáciu informácií a kategorizáciu sietí a informačných systémov podľa § 20 ods. 2 Zákona o KB je treba vykonať podľa definovanej klasifikačnej schémy, v súlade so štruktúrou klasifikácie informácií a kategorizácie sietí a informačných systémov podľa prílohy č. 2 Vyhlášky.

1. **Analýza rizík kybernetickej bezpečnosti a návrh na riadenie rizík:**

Riadenie aktív pozostáva z identifikácie a evidencie všetkých:

1. aktív, od ktorých závisí poskytovanie základnej služby,
2. podporných služieb, prostredníctvom ktorých sa zabezpečuje kontinuita základnej služby a jej poskytovanie,
3. zodpovedných osôb za identifikáciu a evidenciu aktív a
4. vlastníkov aktív.

Riadenie rizík pozostáva z:

1. identifikácie zraniteľností,
2. identifikácie hrozieb,
3. identifikácie a analýzy rizík s ohľadom na aktívum,
4. určenia vlastníka rizika,
5. implementácie organizačných a technických bezpečnostných opatrení v závislosti od identifikovaných rizík vrátane informácie, ktoré bezpečnostné opatrenia sú implementované a ktoré bezpečnostné opatrenia nie sú implementované spolu s odôvodnením,
6. analýzy funkčného dopadu,
7. pravidelného preskúmavania identifikovaných rizík a v závislosti od toho aktualizácie prijatých bezpečnostných opatrení.

Identifikácia hrozieb je založená na identifikácii aktív a ich vlastníkov a identifikácii zraniteľností potenciálne pôsobiacich na tieto aktíva.

1. **Plánovanie kontinuity činnosti, vypracovanie návrhu Stratégie kontinuity a vytvorenie plánov kontinuity:**
2. analýza dopadov KB,
3. stratégia kontinuity,
4. vypracovanie plánov kontinuity,
5. testovanie plánov kontinuity.
6. **Identifikácia parametrov potrebných pre výber budúcich dodávateľov technológie alebo služieb v oblasti informačnej a kybernetickej bezpečnosti:**

Táto služba pomáha verejnému obstarávateľovi nezávisle a s odbornou starostlivosťou identifikovať kritéria a podmienky pre obstarávanie technológií a služieb v oblasti informačnej a kybernetickej bezpečnosti od budúcich dodávateľov. Služba bude poskytovaná na vyžiadanie zo strany verejného obstarávateľa v rozsahu najviac 2 MD mesačne počas trvania zmluvného vzťahu.

1. **Zaškolenie a podpora pri implementácií navrhnutých riešení informačnej bezpečnosti a udržiavaní súladu  
   s platnou legislatívou v oblasti kybernetickej bezpečnosti:**
2. zaškolenie zamestnancov verejného obstarávateľa v rozsahu 16 hodín v oblasti legislatívnych požiadaviek a opatrení (zosúladenie zmlúv a internej dokumentácie),
3. zaškolenie zamestnancov verejného obstarávateľa v rozsahu 16 hodín v oblasti technických požiadaviek a opatrení (implementácia navrhnutých technických a bezpečnostných riešení).