Príloha č. 2

Predmet zákazky: ***Zabezpečenie auditu kybernetickej bezpečnosti***

**Opis predmetu zákazky**

Predmetom zákazky je vykonanie auditu kybernetickej bezpečnosti (ďalej len „audit“) podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) v súlade s vyhláškou NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora (ďalej len „vyhláška o audite“) u prevádzkovateľa základnej služby s cieľom overiť plnenie povinností podľa zákona a posúdiť zhodu prijatých bezpečnostných opatrení s požiadavkami podľa zákona a 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“) prevádzkovateľa základnej služby. Auditom sa identifikujú nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby s cieľom prijať opatrenia na ich odstránenie a nápravu.

**Opis predmetu zákazky zahŕňa:**

a) posúdenie kompletnosti údajov potrebných na vykonanie auditu v rozsahu minimálnych náležitostí uvedených v prílohe č. 2 vyhlášky NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora,

b) určenie rozsahu auditu spôsobom podľa prílohy č. 3 vyhlášky NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora ,

c) určenie metódy auditu podľa prílohy č. 4 vyhlášky NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora ,

d) pripravenie podkladov a pracovných dokumentov potrebných na výkon auditu,

e) preskúmanie bezpečnostnej dokumentácie a vyhodnotenie bezpečnostných opatrení v oblastiach:

1. organizácie informačnej bezpečnosti,

2. riadenia aktív, hrozieb a rizík,

3. personálnej bezpečnosti,

4. riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,

5. technických zraniteľností systémov a zariadení,

6. riadenia bezpečnosti sietí a informačných systémov,

7. riadenia prevádzky,

8. riadenia prístupov,

9. kryptografických opatrení,

10. riešenia kybernetických bezpečnostných incidentov,

11. monitorovania, testovania bezpečnosti a bezpečnostných auditov,

12. fyzickej bezpečnosti a bezpečnosti prostredia,

13. riadenia kontinuity procesov;

f) vypracovanie kontrolného záznamu auditovaných bezpečnostných opatrení podľa prílohy č. 4 vyhlášky NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora,

g) vyhodnotenie auditných zistení, oboznámenie prevádzkovateľa základnej služby so zistenými nedostatkami a zostavenie odporúčaných opatrení na ich odstránenie v písomnej forme,

h) vypracovanie a predloženie záverečnej správy o výsledkoch auditu v rozsahu podľa § 2 vyhlášky NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora , ktorá obsahuje najmä:

a) meno, priezvisko, číslo platného certifikátu audítora, dátum vyhotovenia a jeho podpis,

b) vymedzenie rozsahu vykonaného auditu,

c) cieľ auditu,

d) metódy vykonaného auditu,

e) zhrnutie zistení výsledkov auditu a konštatovanie súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov,

f) odporúčané nápravné opatrenia audítora pri zistení nedostatkov,

g) dokumenty, najmä:

1. kópia certifikátu audítora,

2. kópia žiadosti o vykonanie auditu,

3. výpočet rozsahu trvania auditu a zdôvodnenie jeho skrátenia alebo predĺženia,

4. kontrolný záznam s vyjadrením prevádzkovateľa základnej služby so zisteniami auditu,

5. harmonogram auditu,

6. zoznam posúdenej dokumentácie,

7. uvedenie a zdôvodnenie zmien a rozdielov priebehu auditu oproti plánovanému harmonogramu,

8. zhodnotenie plnenia povinností podľa zákona a celkového stavu prijatých bezpečnostných opatrení každého informačného systému súvisiaceho so základnou službou, vyslovenie súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov a konkrétne uvedenie nedostatkov.

**Úspešný uchádzač je povinný začať s vykonávaním auditu kybernetickej bezpečnosti v termíne do 2 pracovných dní od účinnosti zmluvy o vykonaní auditu. Úspešný uchádzač je povinný vykonať audit a predložiť záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti do 31. októbra 2021. Predpokladaný termín vykonania certifikačného auditu je október 2021.**

**Minimálne náležitosti k vykonaniu auditu kybernetickej bezpečnosti podľa prílohy číslo 2. vyhlášky NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.**

Verejný obstarávateľ požaduje vykonanie auditu prostredníctvom certifikovaného audítora kybernetickej bezpečnosti podľa vyhlášky NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

- Čestné vyhlásenie uchádzača, že nekoná v rozpore s vyhláškou NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

**Úspešný uchádzač je povinný do tretieho pracovného dňa nasledujúceho po dni nadobudnutia účinnosti Zmluvy predložiť Objednávateľovi na schválenie vypracovaný organizačný a časový harmonogram výkonu auditu, ktorého súčasťou bude identifikácia organizačných útvarov, procesov, auditovaných sietí a informačných systémov a fyzických lokalít Prevádzkovateľa základnej služby s uvedením jednotlivých časových úsekov auditu.**

**DOPLNENIE:**

K určeniu rozsahu auditu KB spôsobom podľa **prílohy č. 3 vyhlášky NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora :**

\* Počet služieb verejného obstarávateľa zaradených do zoznamu základných   
služieb: zdravotná starostlivosť, laboratórne služby

\* Ste prevádzkovateľom prvku kritickej infraštruktúry? Áno

\* Počet informačných systémov s väzbou na základné služby: 10

\* Počet zamestnancov (používateľov základných služieb): 800

\* Počet pracovníkov zúčastňujúcich na prevádzke IS a zabezpečovaní   
bezpečnostných opatrení podľa vyhlášky č.362/2018 Z.z. (interní a   
externí): 50- z toho interní - 13, externí - 37.

\* Počet externých pracovísk, kde je prevádzkovaný samostatný IS s väzbou   
na základnú službu, iný ako na ostatných pracoviskách? 0

\* Počet tretích strán zúčastňujúcich sa na prevádzke IS: 8

\* Vlastní verejný obstarávateľ platný certifikát ISMS?  nie

\* Odhadovaný počet externých zaregistrovaných používateľov základných   
služieb: nevieme o takých

\* Má verejný obstarávateľ zaregistrovaný aspoň jeden informačný systém   
kategórie III? áno

\* Ak nie, sú všetky IS zaradené v kategórii I? nie

\* Vyskytol sa u Vás za posledné 2 roky závažný kybernetický bezpečnostný   
incident? nie

\* Porušili ste povinnosti podľa ZoKB, prípadne bola uložená pokuta za   
porušenie povinnosti podľa zákona č. 69/2018 Z. z.? nie