

Opis predmetu zákazky

Predmetom verejného obstarávania je obstaranie služieb auditu kybernetickej bezpečnosti s cieľom preveriť účinnosť prijatých bezpečnostných opatrení verejného obstarávateľa a plnenie požiadaviek stanovených zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti v platnom znení (ďalej len „Zákon“), príslušnej Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z.z. (ďalej len „Vyhláška o bezpečnostných opatreniach“), ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení a Vyhlášky Národného bezpečnostného úradu č. 493/2022 Z.z. (ďalej len „Vyhláška o audite“) o audite kybernetickej bezpečnosti.

Uchádzač sa v rámci auditu kybernetickej bezpečnosti zaväzuje zabezpečiť výkon auditu

prostredníctvom certifikovaného audítora kybernetickej bezpečnosti (ďalej len „Audítor kybernetickej bezpečnosti“) podľa Vyhlášky o audite, ktorý spĺňa všetky požiadavky na výkon auditu.

Predmet zákazky sa bude považovať za splnený riadne a včas dňom predloženia Záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti.

Uchádzač sa v rámci auditu kybernetickej bezpečnosti zaväzuje poskytnúť nasledovné služby:

a) v súlade so Štandardom na výkon auditu kybernetickej bezpečnosti vydanom Kompetenčným centrom kybernetickej bezpečnosti (ďalej len „Metodika auditu“) a v súlade s požiadavkami Zákona a Vyhlášky o bezpečnostných opatreniach výkon auditu kybernetickej bezpečnosti, a teda auditu sietí a informačných systémov verejného obstarávateľa ako prevádzkovateľa základnej služby, s cieľom preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek Zákona a Vyhlášky o bezpečnostných opatreniach, ktoré definujú príslušné požiadavky na prevádzkovateľa základnej služby. Audit kybernetickej bezpečnosti zahŕňa tieto požiadavky:

Posúdenie prijatia a dodržiavania všeobecných bezpečnostných opatrení vo forme úloh, procesov, rolí a technológií v organizačnej, personálnej a technickej rovine v oblastiach:

- a) organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
- b) riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
- c) personálnej bezpečnosti,
- d) riadenia prístupov,
- e) riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
- f) bezpečnosti pri prevádzke informačných systémov a sietí,
- g) hodnotenia zraniteľností a bezpečnostných aktualizácií,
- h) ochrany proti škodlivému kódu,
- i) sieťovej a komunikačnej bezpečnosti,

Príloha č.1

- j) akvizície, vývoja a údržby informačných sietí a informačných systémov,
- k) zaznamenávania udalostí a monitorovania,
- l) fyzickej bezpečnosti a bezpečnosti prostredia,
- m) riešenia kybernetických bezpečnostných incidentov,
- n) kryptografických opatrení,
- o) kontinuity prevádzky,
- p) auditu, riadenia súladu a kontrolných činností.

Verejný obstarávateľ poskytne uchádzačovi všetky informácie a súčinnosť potrebnú pre splnenie predmetu zákazky.

Výstupom auditu kybernetickej bezpečnosti je Záverečná správa o výsledkoch auditu kybernetickej bezpečnosti v slovenskom jazyku (ďalej aj ako „Správa“) vypracovaná v súlade s požiadavkami Vyhlášky o audite. Správa bude mať nasledovnú štruktúru, pokiaľ z Vyhlášky o audite nevyplýva iná štruktúra a rozsah:

- (a) Meno, priezvisko a číslo platného certifikátu audítora, dátum vyhotovenia a podpis audítora,
- (b) Vymedzenie rozsahu vykonaného auditu kybernetickej bezpečnosti,
- (c) Cieľ auditu kybernetickej bezpečnosti,
- (d) Použité postupy a metodiky vykonaného auditu kybernetickej bezpečnosti,
- (e) Zhrnutie zistení výsledkov auditu kybernetickej bezpečnosti a konštatovanie súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov,
- (f) Odporúčané nápravné opatrenia audítora pri zistení nedostatkov,
- (g) Dokumenty, ktorými sú najmä:
 1. Kópia certifikátu audítora,
 2. Kópia žiadosti o výkon auditu podľa prílohy č. 1 Vyhlášky o audite,
 3. Výpočet rozsahu trvania auditu a zdôvodnenie skrátenia alebo predĺženia,
 4. Kontrolný záznam auditovaných bezpečnostných opatrení 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.

Verejný obstarávateľ prikladá Žiadosť o vykonanie auditu kybernetickej bezpečnosti podľa prílohy č. 1 vyhlášky Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora. Minimálne náležitosti sú uvedené v žiadosti o audit kybernetickej bezpečnosti.

Žiadosť o audit kybernetickej bezpečnosti:

1. Identifikácia prevádzkovateľa základnej služby:
Slovenská agentúra životného prostredia, Tajovského 28, 975 90 Banská Bystrica
2. Identifikácia základných služieb podporených auditovanými informačnými systémami a sieťami:

Správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

3. Počet zamestnancov prevádzkovateľa základnej služby:
290 zamestnancov
4. Minimálne technické a funkčné parametre prevádzky základných služieb:
 - a. Počet služieb verejného obstarávateľa zaradených do zoznamu základných služieb: 1
 - b. Počet informačných systémov s väzbou na základné služby: 10
 - c. Počet zamestnancov : 290
 - d. Počet pracovníkov zúčastňujúcich na prevádzke IS (interní a externí): 23
 - e. Počet lokalít: 3
 - f. Počet tretích strán zúčastňujúcich na prevádzke IS: 1
 - g. Verejný obstarávateľ nie je zapojený do siete Govnet
 - h. Verejný obstarávateľ nevlastní platný certifikát ISMS.
 - i. SAŽP má zaregistrovaný informačný systém kategórie II.
 - j. V SAŽP sa za posledné 2 roky nevyskytol závažný kybernetický bezpečnostný incident.
 - k. V SAŽP nebol vykonaný audit kybernetickej bezpečnosti ani nebola uložená pokuta za porušenie povinnosti podľa zákona č. 69/2018 Z. z.

5. Meno, priezvisko a kontaktné údaje zodpovedného zamestnanca prevádzkovateľa základnej služby, ktorý poskytne audítorovi počas výkonu auditu požadovanú súčinnosť a bude ho sprevádzať:
Martin Podhorec – Manažér kybernetickej a informačnej bezpečnosti,
Marek Andel – Vedúci odboru prevádzky IT,