Špecifikácia požiadavky – podrobný opis predmetu zákazky: zavedenie opatrení podľa zákona 69/2018 Z. z. o kybernetickej bezpečnosti a zákona 95/2019 Z. z. o informačných technológiách verejnej správy

1.Vykonanie GAP analýzy v zmysle zákona 95/2019 Z. z., č. 69/2018 Z. z. a vyhlášky č. 362/2018 Z. z

Požadujeme vykonanie GAP (rozdielovej) analýzy zákona č. 69/2018 Z. z., vyhlášky č. 362/2018 Z. z. a zákona č. 95/2019 Z. z., v nasledujúcich oblastiach:

- politika informačnej bezpečnosti,
- organizácia informačnej bezpečnosti,
- personálna bezpečnosť,
- riadenie aktív,
- riadenie prístupov,
- kryptografia,
- fyzická bezpečnosť a bezpečnosť prostredia,
- bezpečnosť prevádzky,
- komunikačná bezpečnosť,
- akvizícia, vývoj a údržba informačných systémov,
- riadenie vzťahov s dodávateľmi,
- riadenie incidentov informačnej bezpečnosti,
- aspekty informačnej bezpečnosti v riadení kontinuity,
- súlad s právnymi a zmluvnými požiadavkami.

Počas kontroly požadujeme identifikovať rozdiely voči definovaným požiadavkám legislatívy vo vyššie uvedených oblastiach. Požadovaným výstupom kontroly bude zoznam nezhôd s vyhláškou 362/2018 Z. z..

2.Vykonanie testu siete

Test siete musí zahŕňať jej sken so zameraním na :

- zistenie zapojených zariadení v sieti (aktívne prvky, PC, servery),
- zistenie zraniteľností na zariadeniach v sieti podľa CVE databázy,
- otestovanie na prítomnosť základných (predvolených) hesiel.

Výstupom je manažérsky a podrobný popis nájdených zraniteľností podľa ich závažnosti a ich klasifikácia.

3.Vykonanie rizikovej analýzy

Požadujeme vypracovanie rizikovej analýzy v nasledovnom rozsahu:

- identifikácia informačných aktív
- kategorizácia informačných aktív
- ohodnotenie a kategorizácia aktív,
- identifikácia zraniteľností,
- identifikovanie hrozieb,
- hodnotenie rizík vyplývajúcich z hrozieb a zraniteľností,
- správa a návrhy na odstránenie vysokých rizík.

Výstupom tejto analýzy je zoznam kľúčových aktív a ich hodnotenie a dokument, ktorý popisuje súlad stavu prostredia zákazníka s požiadavkami zákona o ITVS a ZoKB (vrátane návrhu opatrení).

Riziková analýza musí slúžiť ako podklad na vypracovanie bezpečnostného projektu v zmysle zákona 95/2019 Z. z. a zákona č. 69/2018 Z. z.

4.Bezpečnostná dokumentácia

Na základe zistených nezrovnalostí a návrhov opatrení v kontrole požadujeme vypracovať bezpečnostnú dokumentáciu tak, aby bola v súlade so zákonmi č. 69/2018 Z. z. a č.95/2019 Z. z. a tým aj spĺňala požadované bezpečnostné kritéria zákona o kybernetickej bezpečnosti a zákona o informačných systémoch verejnej správy a boli pripravený na audit.

Vypracovaná dokumentácia musí obsahovať:

- Bezpečnostná stratégia kybernetickej bezpečnosti
- Zdokumentovanie IT aktív a ich vlastníkov – zákon č. 95/2019 Z. z., č. 69/2018 Z. z.
- Bezpečnostné politiky
    - Organizácia informačnej bezpečnosti
    - Politika informačnej bezpečnosti,
    - Riadenie bezpečnostných rizík
    - Riadenie incidentov informačnej bezpečnosti
    - Riadenie informačných aktív
    - Pravidlá správania a dobrej praxe
    - Riadenie dodávateľských vzťahov
    - Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií
    - Riadenie a prevádzka informačno-komunikačných technológií
    - Riadenie prístupov
    - Kryptografia
    - Riadenie súladu
    - Riadenie kontinuity procesov a činností
- Smernice na riešenie bezpečnostných incidentov (Procedúra, Zodpovednosti, Postupy)
- Interný riadiaci akt alebo Bezpečnostný projekt ITVS
- Klasifikácia informácií a kategorizácia sietí a informačných systémov podľa § 4 vyhlášky č. 362/2018 Z. z.

5.Implementácia bezpečnostnej dokumentácie

V rámci implementácie bezpečnostnej dokumentácie požadujeme jej formou školenia, navrhovania nových procesov, vytvorenia dokumentácie a odporúčania potrebných opatrení na základe vykonaných analýz a našich pripomienok a požiadaviek. Dokumentácia musí vyhovovať týmto požiadavkám a zároveň musí spĺňať požiadavky legislatívy.

Pre implementáciu bezpečnostnej politiky budú vytvorené základné metodické a procesné dokumenty, ktoré aplikujú tieto časti:

- Deklarácia vedenia organizácie k bezpečnosti ITVS a kybernetickej bezpečnosti - ochrana informácií
    - Stanovenie cieľov IB v organizáci
    - Stratégia kybernetickej bezpečnosti
    - Nastavenie podpory vedenia organizácie pri ich napĺňaní
    - Oblasť použiteľnosti bezpečnostnej politiky
    - Vyhlásenie o zavedení opatrení
- Štruktúra a obsah bezpečnostnej dokumentácie nadväzujúcej na bezpečnostnú politiku
- Stanovenie zodpovednosti zamestnancov za presadzovanie a dodržiavanie bezpečnostnej politiky
- Implementácia smerníc a predpisov formou školenia alebo návrhom opatrení.
- Školenie zamestnancov
- Vypracovanie koncepcie rozvoja – zákon č. 95/2019 Z. z.

Implementácia spĺňa požiadavky definované v § 5 vyhlášky č. 362/2018 Z. z..

Cieľom je vytvoriť organizačné podmienky pre zavedenie a riadenie informačnej bezpečnosti v organizácii.

6.Podpora

Požadujeme od Vás starostlivosť spojenú s otázkami ohľadom kybernetickej bezpečnosti, ktoré zabezpečuje:

- v prípade potreby konzultácie a poradenstvo pri imlementácii opatrení.
- možnosť opráv v prípade reklamácie,
- osobné stretnutia a návštevy,
- kompletné zaškolenie zamestnancov k bezpečnosti ITVS a kybernetickej bezpečnosti v priestoroch MiÚ MČ Karlova Ves alebo online formou.

7.Ostatné

Ak si uchádzač spoplatňuje aj daľšie aktivity súvisiace s realizáciou zákazky (napr. dopravné náklady), potrebné je ich uviesť v tejto časti.

V zmysle zákona o ITVS požadujeme vykonať potrebné aktivity a vypracovať dokumentáciu pre všetky rozpočtové a príspevkové organizácie mestskej časti, ktoré spadajú pod IČO mestskej časti.

Uchádzač odovzdá všetky požiadavky a podmienky pre začatie realizácie tejto zákazky.

Požadujeme uviesť fixnú cenu zákazky bez DPH a s DPH.

Uchádzač predloží ako doklad odbornej spôsobilosti:

- Certifikát zavedenia systému manažérstva podľa ISO/IEC 27001:2013 pre oblasť informačnej a kybernetickej bezpečnosti.
- Certifikát „Certified Information Security Manager (CISM)“ alebo „Certified Information System Auditor (CISA)“
- Certifikát „ ISO/IEC 27001:2013 Internal Auditor“ alebo, certifikát „ISO/IEC 27001 Lead Auditor“
- Predloženie minimálne 3 referencií zavedenia požiadaviek zákonov č. 69/2018 Z. z. a č. 95/2019 Z. z. z oblasti verejnej správy Slovenskej republiky.