1. pielikums

cenu aptaujai “IT auditu Talsu novada pašvaldība vajadzībām”,

identifikācijas Nr. TNPz 2022/98

**TEHNISKĀ SPECIFIKĀCIJA – DARBA UZDEVUMS**

**Veicamie darba uzdevumi un esošās situācijas analīze, kur ietverta:**

1. IT infrastruktūras izpēte:
   1. ikdienas kritisko procesu apzināšana, infrastruktūras izpēte;
   2. organizācijas struktūras izpēte un kritisko sistēmu identificēšana;
   3. tīkla topoloģijas izpēte;
   4. esošās IT dokumentācijas un citu ar IT pārvaldību saistīto normatīvo aktu izpēte un nepilnību identificēšana atbilstoši Pasūtītāja nepieciešamībām, kā arī dokumentācijas pilnveidošana un izveidi, ja nepieciešams, IT audita gaitā ar darba veicēja iesaisti.
2. Koplietošanas elementu (IS, infrastruktūra, darbstaciju, serveru telpas) izpēte, pārbaude un analīze:
   1. Pasūtītājam ir ~150 darbstacijas un 3 fiziski serveri un 7 virtuālie serveri (Windows un Linux), jāveic vismaz 4 tipveida pārbaudes, t. sk. konfigurācijas novērtējums industrijas labākajai praksei, drošības pasākumu analīze;
   2. papildsistēmu darbības analīze, piemēram, rezerves kopijas, koplietošanas diski;
   3. Windows grupu politiku, lietotāju kontu analīze un atbilstība;
   4. IS atbilstība normatīvajiem aktiem (Informācijas tehnoloģiju drošības likums, Ministru kabineta noteikumi Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”, Pasūtītāja iekšējie normatīvie akti);
   5. tīkla infrastruktūras un iekārtu drošības pasākumu izpēte un novērtējums;
   6. serveru telpas drošības atbilstības novērtējums;
   7. datu drošības novērtējums – glabāšana, pārraide, dzēšana;
   8. iekšējā tīkla un ārējo IP adrešu iespējamo drošības ievainojamību identificēšanu ar automatizētu rīku;
   9. pārbaudei jāietver vismaz 4 Pasūtītāja nosaukto tīmekļvietņu specifisko ievainojamību identificēšana un padziļināta pārbaude (identificēt application level ievainojamības, konfigurācijas nepilnības u.c. drošības faktorus, kas ietekmē programmas kiberaizsardzības spējas; norādīt iespējamos uzlabojumus, noteikt atbilstību OWASP Top 10 2017 un citām ievainojamībām).
3. Noslēguma ziņojums:
   1. noslēguma ziņojumam ir jābūt detalizētam par visām veiktajām pārbaudēm, kas ietver visus novērojumus, identificētos trūkumus, tos kategorizējot pēc riska līmeņiem, novēršanas prioritātes, un rekomendācijām tos novērst vai mazināt, t. sk. fiziskus un virtuālus;
   2. noslēguma ziņojumā obligāti jāietver serveru telpas atbilstība, fizisko iekārtu un papildsistēmu darbības analīze un ar to saistīto procesu analīze;
   3. tīkla infrastruktūras darbības analīze;
   4. Wi-Fi infrastruktūras novērtēšana (drošība, veiktspēja, piekļuve un ieteikumi uzlabojumiem);
   5. operētājsistēmu, t. sk. kontu pārvaldības darbības analīze;
   6. lietojumprogrammatūru analīze;
   7. datu drošība un ar to saistītās dokumentācijas analīze.
   8. par IT audita rezultātā sagatavoto noslēguma ziņojumu Izpildītājs sniedz Pasūtītājam prezentāciju 30 min – 1 h garumā pušu iepriekš savstarpēji saskaņotā laikā.
4. Izstrādāt IT dokumentāciju atbilstoši Ministru kabineta noteikumu Nr.442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām” prasībām:
   1. Sistēmas drošības politika;
   2. Sistēmas drošības iekšējie noteikumi;
   3. Sistēmu lietošanas noteikumi;
   4. Sistēmas darbības atjaunošanas plāns (Izpildītājs izstrādā vadlīnijas un konsultē plāna detalizētā izstrādē).