Pakkumuse esitamise ettepaneku
Lisa 1

Aktsiaselts Tallinna Linnatransport
Väikehange: „Küberturbeaudit“

TEHNILINE KIRJELDUS

1. Hanke ese

Aktsiaselts Tallinna Linnatransport (edaspidi TLT ja/või Hankija) otsib koostööpartnerit, et viia läbi põhjalik küberturbeaudit (edaspidi audit). Audit peab andma ülevaate TLT küberturvalisuse olukorrast hetkeseisuga, tuvastama võimalikud turvanõrkused IT-infrastruktuuris- ja infosüsteemides. Audit peab sisaldama soovitusi küberturvalisuse parandamiseks vastavalt rahvusvahelistele standarditele ja parimatele praktikatele.

2. Hanke eesmärk

2.1. Audit peab saavutama järgmised eesmärgid:

2.1.1. Hinnata TLT praegust küberturbe küpsustaset.

2.1.2. Tuvastada tehnilised- ja organisatsioonilised turvanõrkused.

2.1.3. Anda soovitusi turvanõrkuste kõrvaldamiseks ja küberturvalisuse taseme tõstmiseks.

2.1.4. Koostada tegevuskava tuvastatud probleemide lahendamiseks.

2.1.5. Arenguplaan ja järjepidev tugi: Peale auditi läbiviimist ootame pakkujalt arenguplaani, mis sisaldab konkreetseid soovitusi tuvastatud nõrkuste kõrvaldamiseks ning ettepanekuid küberturvalisuse taseme tõstmiseks. Hindame pakkujaid, kes suudavad pakkuda järjepidevat tuge ja nõustamist arenguplaani elluviimisel.

2.1.6. Eelistame pakkujaid, kes suudavad pakkuda CISOaaS teenust hilisemalt auditi põhjal tehtud tegevuskava läbiviimiseks.

3. Hanke esemele ja pakkujale esitatavad nõuded

3.1. Audit peab hõlmama järgmisi valdkondi:

3.1.1. Infovarade kaardistamine ja klassifitseerimine *s.h. IOS ja Android rakendused*;

3.1.2. Tehniliste turvanõrkuste skaneerimine, sealhulgas perimeetri, sisevõrgu ja veebirakenduste turvalisus;

3.1.3. Küberturbe poliitikate, protsesside ja dokumentatsiooni ülevaatus;

3.1.4. Töötajate küberturvalisuse teadlikkuse hindamine;

3.1.5. Füüsiline turvalisus, sealhulgas serveriruumide ja andmekeskuste turvalisus;

3.1.6. Digitaalse jalajälje analüüs, sealhulgas tumeveebi skaneerimine;

3.1.7. Aruandlus, mis sisaldab kõikide leidude dokumenteerimist ja soovituslikku tegevuskava.

3.1.7.1. Aruandes tuleb kirjeldada kõiki uuritud valdkondi, nagu infovarade kaardistamine, turvanõrkuste skaneerimine, küberturbe poliitikate läbivaatus, töötajate teadlikkuse hindamine, füüsiline turvalisus ja digitaalse jalajälje

analüüs. Iga valdkonna kohta tuleks esitada üksikasjalikud tulemused ja tuvastatud nõrkused või probleemid.

3.1.7.2. Lisaks leidude kirjeldamisele peab aruanne sisaldama konkreetseid soovitusi tuvastatud nõrkuste kõrvaldamiseks ning küberturvalisuse taseme tõstmiseks. Soovitused peaksid olema praktilised ja teostatavad, ning lisaks ka tegevuskava nende elluviimiseks.

3.1.7.3. Aruanne tuleks esitada loetavas ja professionaalses vormis. Kasutada selget struktuuri, mis võimaldab kiiresti leida aruandes sisalduvat teavet.

3.1.7.4. Aruandes tuleks lisada ka tõendid uurimiste ja analüüside kohta, nagu logifailid, skaneerimise tulemused ja ekraanitõmmised.

3.1.7.5. Kuna aruanne sisaldab tundlikku teavet, tuleb tagada selle konfidentsiaalsus. Aruannet tuleks jagada ainult autoriseeritud isikutega ja kasutada turvalisi vahendeid selle edastamiseks.

3.2. Pakkuja peab omama vähemalt 5 aastat kogemust küberturbeauditite läbiviimisel.

3.3. Pakkuja ettevõte peab omama ISO27001 sertifikaati.

3.4. Pakkuja meeskond peab omama ühte tehnilist küberturbealast sertifikaati: CISSP, CE, või CND.

3.5. Pakkuja peab omama vähemalt 3 lõpetatud projekti viimase 3 aasta jooksul, mis on teostatud organisatsioonidele, kus töötajate arv on vähemalt 250 inimest. Projektid peavad hõlmama küberturvalisuse auditeid või sarnaseid teenuseid, mis on otseselt seotud IT-turvalisusega.

3.6. Audit raport peab olema esitatud eesti keeles.

3.7. Audit tuleb läbi viia ja lõppraport esitada 2 kuu jooksul alates hankelepingu sõlmimisest.