HANKELEPING nr 3-9/3179-16

Tervise ja Heaolu Infosüsteemide Keskus (edaspidi tellija), registrikood 70009770, aadress Pärnu mnt 132, 1317 Tallinn, keda esindab põhimääruse alusel direktor Margus Arm
ja
Clarified Security OÜ (edaspidi täitja), registrikood 12164540, asukoht Lõõtsa 12, 11415, Tallinn, keda esindab seaduse ja põhikirja alusel juhatuse esimees Mehis Hakkaja, edaspidi ka pool või pooled, sõlmisid käesoleva hankelepingu (edaspidi leping) alljärgnevas:

1 Lepingu sõlmimise alus ja ese

1.1 Leping sõlmitakse riigihangete seaduse § 30 alusel, lähtudes täitjaga sõlmitud raamlepingust nr 4.2-3/2266-1.
1.2 Tööde detailsem kirjeldus on toodud lepingu lisas 1 „Teenuse kirjeldus“.
1.3 Lepingu lahutamatuteks osadeks on tellija „Infosüsteemide turvalisuse testimine II“ (viitenumber 246996) riigihanke alusdokumendid, tellija tellimus, täitja pakkumus ning arvestades antud lepingus kokkulepitud erisused.
1.4 Kõik lepingu muudatused sõlmitakse lepingu lisadena, mis jõustuvad pärast nende allkirjastamist mõlema poole poolt või poolte määratud tähtajal.

2 Lepingu maksumus ja maksetingimused

2.1 Lepingu kogumaksumus on kuni 30 000 (kolmkümmend tuhat) eurot, millele lisandub käibemaks (edaspidi lepingu maksumus). Lepingu maksumus sisaldab kõiki lepingu täitmiseks vajalikke kulusid.[1]
2.1.1 Ühe töötunni maksumus on 120 (ükssada kakskümmend) eurot, millele lisandub käibemaks.
2.2 Lepingut rahastatakse projektist „Personaalmeditsiini rakendamine Eestis“ (kood: 2014-2020.12.03.19-0561). Tulemi teostamisel lähtutakse https://www.riigiteataja.ee/akt/102062021021?leiaKehtiv ja https://www.sm.ee/sites/default/files/tat_terviktekst.pdf sätestatust.
2.3 Tööd antakse üle ühes etapis vastavalt Lisa 1 Tehnilises kirjelduses punktile 4.5.

3 Lepingu kehtivus ja lõpetamine

3.1 Leping jõustub hetkel, mil pooled on lepingu allkirjastanud ning kehtib 3 kuud lepingu sõlmimisest või lepingust tulenevate kohustuste täitmiseni, vastavalt varem saabunud asjaolule.
3.2 Tellija võib lepingu 10 (kümne) kalendripäevase etteteatamistähtajaga olenemata põhjusest üles öelda ning sellisel juhul on täitjal õigus nõuda tasu vaid lepingu ülesütlemise hetkeks faktiliselt tehtud tööde eest.
3.3 Täitjal on õigus lõpetada leping ennetähtaegselt, teatades sellest tellijale kirjalikult ette vähemalt 2 (kaks) nädalat, kui tellija keeldub nõuetekohaselt valmistatud tööde eest tasu maksmisest.
3.4 Ülaltoodud alustel lepingu ennetähtaegsel lõpetamisel on täitjal õigus tellijalt sisse nõuda tasu lepingu lõpetamise hetkeks faktiliselt tehtud tööde eest.

[1] Punktid 2.1 – 2.3 täpsustatakse tellimuse käigus.

4 Kontaktisikud

4.1 Tellija kontaktisik on Bret Rand (tel: 53 004 411, e-post: bret.rand@tehik.ee);

4.2 Täitja kontaktisik on Mehis Hakkaja (tel: 603 6644, e-post: mehis@clarifiedsecurity.com).

5 Lõppsätted

5.1 Kõik lepingu muudatused sõlmitakse lepingu lisadena, mis jõustuvad pärast nende allkirjastamist mõlema poole poolt.

5.2 Käesoleva lepingu täitmisel tekkivad vaidlused ja lahkarvamused lahendavad pooled läbirääkimiste teel. Kokkuleppe mittesaavutamisel lahendatakse vaidlused Harju Maakohtus.

5.3 Leping on allkirjastatud digitaalselt.

6 Lisad

6.1 Käesoleva lepingu lahutamatuteks lisadeks on (ei allkirjastata koos hankelepinguga):

6.1.1 Lisa 1 – Tehniline kirjeldus;

6.1.2 Lisa 2 - Tellimus;

6.1.3 Lisa 3 - Pakkumus.

Lisa 1

TEENUSE KIRJELDUS

Hanke eesmärgiks on tellija poolt tellitavate, olemasolevate ja valitud infosüsteemide turvalisuse testimine OWASP (Open Web Application Security Project) ASVS (Application Security Verification Standard) versioon 3.0.1 (või juhul kui sõlmitava raamlepingu kehtivuse perioodil peaks eksisteerima uuem versioon, siis uuemale) tasemetele 2 ja 3 vastavate turvatestide teostamine.

Turvatestimise käigus tuleb metoodiliselt testida ja hinnata kõiki potentsiaalseid turvavigu (sealhulgas OWASP Top Ten) ning need tuleb testiraportis detailselt välja tuua koos võimalike lahenduste ja soovitustega, st leitud vigade puhul välja tuua võimalikud ohustsenaariumid.

Testimisel tuleb kontrollida, et testitavate infosüsteemide võimalike haavatavuste kaudu ei oleks võimalik juurde pääseda andmetele, mis asuvad väljaspool testitava rakenduse funktsionaalsust. Testimine hõlmab ka kasutajate horisontaalset ja vertikaalset õiguste ületamise turvatestimist.

Kõik testimised ja lähtekoodi kontrollid tuleb teostada ka käsitsi, sest testitavad süsteemid ei pruugi automaatsete vahenditega testimisel tõepäraseid tulemusi anda. Testimise lõppedes edastab täitja testitavate toodete/lahenduste testiraportid, krüpteerituna tellijale.
Turvatestimised viiakse läbi arendus- või testkeskkondades, kui ei ole kokku lepitud teisiti. Vajadusel luuakse tellija ja testija süsteemide vahele turvatud kanal infosüsteemidele ligipääsemiseks.

Testimise läbiviimiseks peab täitja esitama tellijale IP aadressid, millelt hakatakse turvateste läbi viima. Tellija avab ligipääsu vastavatelt IP aadressidelt testitavatele süsteemidele. Vajadusel teeb tellija ka vajalikud testkasutajad.
Lõppraport tuleb vormistada vastavalt OWASP ASVS reeglitele.