VPD KAROLIS

978800

ATLYGINTINŲ PASLAUGŲ SUTARTIS Nr. APS-520000-1526

Vilnius, 2016-11-04

UAB „IO projects“, pagal Lietuvos Respublikos įstatymus įsteigta ir veikianti įmonė, juridinio asmens kodas 302444537, kurios registruota buveinė yra P. Lukšio g. 32, LT-08222 Vilnius, duomenys apie įmonę kaupiami ir saugomi Lietuvos Respublikos Juridinių asmenų registre, atstovaujama direktoriaus Igno Griškevičiaus, veikiančio pagal įmonės įstatus ir UAB „FortConsult“, pagal Lietuvos Respublikos įstatymus įsteigta ir veikianti įmonė, juridinio asmens kodas 302663666, kurios registruota buveinė yra Kareivių g. 19-187, LT-09133 Vilnius, duomenys apie įmonę kaupiami ir saugomi Lietuvos Respublikos Juridinių asmenų registre, atstovaujama direktorės Zojos Antuchevič, veikiančios pagal įmonės įstatus, 2016-07-20 jungtinės veiklos sutarties Nr. 20160720JVS pagrindu veikiančios įmonės, atstovaujamos įgaliotojo partnerio UAB „IO projects“ direktoriaus Igno Griškevičiaus (toliau – **„Paslaugų teikėjas“**), ir

Vilniaus universitetas, įmonės kodas 211950810, PVM mokėtojo kodas LT119508113, registruotas LR juridinių asmenų registre adresu Universiteto 3, Vilnius, LT-01513, atstovaujama kanclerio Gedimino Miškinio, veikiančio pagal Vilniaus universiteto rektoriaus 2016-02-22 įgaliojimą Nr. 10000-SR-265, (toliau – **„Klientas“**),

toliau Paslaugų teikėjas ir Klientas kiekvienas atskirai gali būti vadinami **„Šalimi“**, o abu kartu – **„Šalimis“**.

Šalys sudarė šią sutartį (toliau – Sutartis) vadovaujantis supaprastinto atviro pirkimo „**VUSIS saugos atitikties ir pažeidžiamumo vertinimo paslaugų pirkimas VU3220**“, CVP IS Nr. 175593, rezultatais ir susitarė dėl toliau išvardytų sąlygų.

1. Sutarties objektas

1.1. Paslaugų teikėjas įsipareigoja suteikti Klientui Sutarties priede Nr. 1 nurodytas ir reikalavimus atitinkančias **VUSIS saugos atitikties ir pažeidžiamumo vertinimo paslaugas** (toliau – Paslaugos), o Klientas įsipareigoja sumokėti už jas Sutarties 2.1. punkte nurodytą kainą.

2. Kaina

2.1. Sutarties (Paslaugų) kaina yra **7 865,00 EUR su PVM**.

2.2. Sutarties (Paslaugų) kaina yra fiksuota, apima visas išlaidas bei visus mokesčius, įskaitant PVM, kuris sudaro 1 365,00 EUR.

3. Paslaugų teikimo terminai

3.1. Paslaugos turi būti suteiktos iki 2016 m. gruodžio 1 d.

3.2. Sutarties šalims pasirašius susitarimą, Paslaugų teikimo terminas gali būti pratęstas 1 kartą, bet ne ilgiau kaip 1 mėnesiui.

4. Mokėjimo sąlygos ir terminai

4.1. Kai Paslaugų teikėjas tinkamai suteikia Paslaugas, Klientas ir Paslaugų teikėjas pasirašo Paslaugų perdavimo-priėmimo aktą (Sutarties priedas Nr. 2). Paslaugų perdavimo-priėmimo aktą iš Kliento pusės turi teisę pasirašyti Klientas ir Sutarties 6 dalyje nurodytas Kliento atstovas.

4.2. Už tinkamai suteiktas Paslaugas Klientas įsipareigoja sumokėti Paslaugų teikėjui Paslaugų kainą (Sutarties 2.1. punktas) per 30 (trisdešimt) kalendorinių dienų nuo Paslaugų perdavimo-priėmimo akto pasirašymo.

5. Šalių atsakomybė

5.1. Klientas, uždelsęs sumokėti Sutarties 4 skyriuje nustatyta tvarka, įsipareigoja Paslaugų teikėjui pareikalavus mokėti 0,05 % dydžio delspinigius nuo laiku neapmokėtos sumos už kiekvieną pradelstą dieną.

5.2. Paslaugų teikėjas, uždelsęs tinkamai suteikti Paslaugas Sutarties 3 dalyje nurodytais terminais, Klientui pareikalavus moka 0,05 % dydžio delspinigius nuo Sutarties kainos, už kiekvieną vėlavimo dieną iki bus pasiekta 1,5 % suma nuo Sutarties kainos.

5.3. Jei delspinigių suma už nesuteiktas ar netinkamai suteiktas Paslaugas pasiekia 1,5 % Sutarties kainos dydžio sumą, Klientas turi teisę Paslaugų teikėjui pritaikyti Sutarties 5.5. punkte nurodyto dydžio baudą, pareikalaudamas ją sumokėti arba išskaičiuodamas ją iš Paslaugų teikėjui mokėtinos sumos (Sutarties kainos), ir/arba nutraukti Sutartį.
5.4. Delspinigių sumą Klientas turi teisę išskaičiuoti iš Paslaugų teikėjui mokėtinos sumos (Sutarties kainos).
5.5. Paslaugų teikėjas Sutarties įvykdymą užtikrina 10 procentų dydžio bauda nuo bendros Sutarties kainos.

6. Už Sutarties vykdymą atsakingi asmenys
6.1. Sutarties Šalys susirašinėja lietuvių kalba. Visi pranešimai, sutikimai ir kitas susižinojimas, kuriuos Šalis gali pateikti pagal Sutartį, bus laikomi galiojančiais ir įteiktais tinkamai, jeigu yra išsiųsti registruotu paštu ar elektroniniu paštu žemiau nurodytais adresais:

	Kliento atstovas	**Paslaugų teikėjo atstovas**
Vardas, pavardė	Viktoras Bulavas	Žydrūnas Skardžius
Adresas	Saulėtekio al. 9, II-i jung. rūmai, 207 k.	P. Lukšio 32, Vilnius
Telefonas	+370 5 236 6202	+370 52789098
El. paštas	viktoras.bulavas@ittc.vu.lt	Zydrunas.skardzius@ioprojects.lt

6.2. Jei pasikeičia Šalies adresas ir (ar) kiti duomenys, tokia Šalis turi informuoti kitą Šalį pranešdama ne vėliau, kaip prieš 5 darbo dienas.

7. Kitos sąlygos
7.1. Sutartis įsigalioja nuo jos pasirašymo ir galioja iki visiškų įsipareigojimų įvykdymo.
7.2. Bendras Sutarties galiojimo laikas vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo nuostatomis negali būti ilgesnis nei 36 mėnesiai.
7.3. Sutartis gali būti nutraukta raštišku Šalių susitarimu.
7.4. Iškilę ginčai tarp Šalių sprendžiami tarpusavio susitarimu. Tuo atveju, jei tokiu būdu ginčo išspręsti nepavyksta, jis sprendžiamas Lietuvos Respublikos teisės aktų nustatyta tvarka.
7.5. Sutarčiai taikoma Lietuvos Respublikos teisė.
7.6. Sutartis sudaryta dviem lygiaverčiais egzemplioriais lietuvių kalba, po vieną egzempliorių kiekvienai Šaliai.
7.7. Sutarties priedai yra neatskiriamos sudedamosios Sutarties dalys:
7.7.1. Techninė specifikacija – priedas Nr. 1;
7.7.2. Specialistų sąrašas – priedas Nr. 2;
7.7.3. Paslaugų perdavimo–priėmimo aktas – priedas Nr. 3.

8. Juridiniai šalių adresai ir parašai:

KLIENTAS
Vilniaus universitetas,
Įmonės kodas 211950810,
PVM mokėtojo kodas LT119508113,
Adresas: Universiteto 3, Vilnius, LT-01513
A/s LT537300010002460768
AB „Swedbank“
Banko kodas 73000

Kancleris Gediminas Miškinis

(parašas) A. V.

PASLAUGŲ TEIKĖJAS
UAB „IO projects“
Įmonės kodas: 302444537
PVM mokėtojo kodas: LT100005017015
Adresas: P. Lukšio g. 32, LT-08222 Vilnius
A/s: LT437044060007699184
Bankas: AB SEB bankas
Banko kodas: 70440

Direktorius Ignas Griškevičius

(parašas) A. V.

VU Viešųjų pirkimų direkcijos
vyresnysis specialistas
Karolis Urbanavičius

Nr. APS-520000-1526

Sutarties priedas Nr. 1
2016-11-04

TECHNINĖS SPECIFIKACIJOS
I. BENDRA INFORMACIJA PASLAUGŲ TEIKĖJUI

1. Vilniaus universiteto (toliau – Kientas) turimos *studijų informacinės sistemos (*toliau – VUSIS*)* saugos atitikties ir pažeidžiamumo vertinimo paslaugos (toliau – Paslaugos) skirtos užtikrinti saugų VUSIS elektroninės informacijos tvarkymą ir perdavimą vykdant Lietuvos Respublikos teisės aktuose nustatytas Vilniaus universiteto kaip *informacinės sistemos valdytojo ir tvarkytojo* funkcijas.

2. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimo Nr. 716 4.3 punktu ir 4.3.1, 4.3.2, 4.3.3 ir 4.3.4 papunkčiais, VUSIS tvarkoma elektroninė informacija pagal jos svarbą laikoma žinybinės svarbos elektronine informacija. Vadovaujantis minėto aprašo 5.3 punktu, pagal joje apdorojamos elektroninės informacijos svarbos kategoriją, VUSIS priskiriama trečiai informacinių sistemų kategorijai.

3. Vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymo Nr. 1T-71 (1.12) 7.2 punktu bei atsižvelgiant į saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, VUSIS priskiriama antram saugumo lygiui.

4. VUSIS veiklą reglamentuoja šie dokumentai:

4.1. Vilniaus universiteto studijų informacinės sistemos nuostatai, patvirtinti 2009 m. sausio 8 d. Vilniaus universiteto rektoriaus įsakymu Nr. R-7;

4.2. Vilniaus universiteto studijų informacinės sistemos duomenų saugos nuostatai, patvirtinti 2014 m. lapkričio 10 d. Vilniaus universiteto rektoriaus Nr. R-512;

4.3. Vilniaus universiteto studijų informacinės sistemos naudotojų administravimo taisyklės, patvirtintos 2015 m. birželio 26 d. Vilniaus universiteto rektoriaus įsakymu Nr. R-254;

4.4. Vilniaus universiteto studijų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėmis, patvirtintos 2015 m. birželio 26 d. Vilniaus universiteto rektoriaus įsakymu Nr. R-254.

5. Turi būti atliktas išorinis ir vidinis VUSIS saugos atitikties ir pažeidžiamumo vertinimas su įsiskverbimo testavimu. Paslauga turi apimti:

5.1. VUSIS naudojamos fizinės ir virtualios įrangos, sisteminės ir taikomosios programinės įrangos saugos atitikties ir pažeidžiamumo vertinimą ir įsiskverbimo testavimą;

5.2. VUSIS žiniatinklio adresu https://is.vu.lt/ taikomųjų programų saugos atitikties ir pažeidžiamumo vertinimą ir įsiskverbimo testavimą;

5.3. VUSIS tvarkomų duomenų teikimo paslaugų saugos atitikties ir pažeidžiamumo vertinimą ir įsiskverbimo testavimą;

5.4. VUSIS įsiskverbimo testavimo, saugos atitikties ir pažeidžiamumo vertinimo ataskaitų parengimą.

II. BENDRIEJI REIKALAVIMAI PASLAUGOMS IR PROJEKTO VALDYMUI

6. VUSIS saugos atitikties ir pažeidžiamumų vertinimas turi būti atliktas vadovaujantis šiais teisės aktais:

6.1. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 (Žin., 2013, Nr. 86-4210);

6.2. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832;

6.3. Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2014 m. gruodžio 18 d. įsakymu Nr. 1T-74.

7. VUSIS įsiskverbimo testavimas turi būti atliktas pagal viešai žinomą ir pripažintą atvirą ar komercinę metodiką. Pasiūlyme turi būti pateiktas pavadinimas, metodikos aprašymas, pakankamas metodikai įvertinti, pasiūlyti ir pagrįsti atakos vektoriai.

8. Paslaugų teikėjas atsakingas už administracinius, darbo grupių organizavimo bei informacijos pateikimo ar sąlygų jai gauti užtikrinimo klausimus. Taip pat jis atsakingas už projekto komunikaciją, projekto rizikų valdymą, dokumentų šablonų suderinimą ir Paslaugų perdavimą.

9. Visi projekto darbai turi būti atliekami pagal su Klientu suderintą kalendorinį Paslaugų teikimo grafiką (projekto planą). Šį grafiką Šalys suderina per tarpusavyje sutartą terminą, bet ne vėliau kaip per 15 dienų nuo Kliento prašymo jį pateikti dienos.

10. Paslaugų teikimo kontrolė bus atliekama vadovaujantis kalendoriniu Projekto (Paslaugų teikimo) planu – grafiku, Paslaugų teikėjui reguliariai pateikiant Klientui suteiktų Paslaugų ataskaitas.

11. Prieš atliekant saugumo ir įsilaužimų testavimus, su Klientu turi būti suderintas ir pasirašytas atskiras planas su Paslaugų teikimo grafiku.

12. Paslaugų teikėjo parengti projekto dokumentai turi būti pateikiami lietuvių kalba.

13. Projekto dokumentai turi būti rengiami ir derinami vadovaujantis šiais reikalavimais:

13.1. Paslaugų teikėjas privalo suderinti su Klientu visų pateikiamų projekto rezultatų formą ir turinį prieš juos pateikdamas Klientui;

13.2. esant poreikiui, turi būti daromi papildomi projekto rezultatų (dokumentų) pakeitimai iki jų priėmimo;

13.3. pateiktų dokumentų projektus Klientas įvertina per 5 darbo dienas nuo pateikimo dienos. Atsižvelgiant į rezultatų apimtį, įvertinimo terminas gali būti keičiamas.

14. Informacinės sistemos saugos reikalavimų atitikties vertinimas pabaigiamas projekto rezultatų pristatymu Klientui ir jo specialistų komandai, per 5 darbo dienas nuo vertinimo ataskaitos pateikimo.

III. VUSIS TAIKOMŲJŲ PROGRAMŲ IR DUOMENŲ TEIKIMO PASLAUGŲ SAUGUMO VERTINIMAS

15. Turi būti atliktas išorinis (angl. Blackbox) VUSIS taikomųjų programų ir duomenų teikimo paslaugų saugumo patikrinimas turint tik minimalias žinias apie testavimo objektus:

15.1. Nustatytos susijusios informacinės sistemos ir įrenginiai bei sudaryta sąsajų schema, pateikiama UML 2, BPMN ar lygiaverčiu formatu;

15.2. Identifikuotos naudojamos technologijos (platforma, programavimo metodai ir priemonės);

15.3. Identifikuotos naudojamos apsaugos priemonės bei kurias iš jų ir kaip galima apeiti;

15.4. Turi būti atliktas rankinis patikrinimas, ar anksčiau automatiniu būdu identifikuoti pažeidžiamumai gali būti pritaikyti realiai, pašalinti klaidingai teigiami rezultatai (angl. False-positive);

15.5. Patikrinti teisių eskalavimo galimybes, kokio lygmens privilegijas sistemoje ir susijusiose duomenų teikimo paslaugose gali gauti įsilaužėlis;

15.6. Patikrinti duomenų teikimo paslaugų pažeidžiamumai (informacijos atskleidimas per klaidų pranešimus ir kita);

15.7. Atliekama pažeidžiamumų paieška (naudotojo autentifikavimo mechanizmo patikrinimas, sesijos vientisumo patikrinimas, įvedamos informacijos apdorojimo patikrinimas, programinio kodo integralumo patikrinimas, klaidų pranešimų apdorojimas, sisteminės informacijos atskleidimas, serviso konfigūravimo klaidos ir pan.) ne mažiau kaip trimis populiariausiais automatizuotais žiniatinklio pažeidžiamumo skeneriais;

15.8. pažeidžiamumų patikrinimas ne mažiau kaip pagal OWASP Application Security Verification Standard 3.0 pirmo lygio reikalavimus (ASVS Level 1), suderintus „OWASP Testing Guide v4“ metodikos punktus (neapsiribojant „OWASP Top 10“ pažeidžiamumais).

16. Turi būti atliktas vidinis (angl. Whitebox) žiniatinklio taikomųjų programų ir žiniatinklio paslaugų saugumo patikrinimas kai užsakovas pateikia informaciją apie testavimo objektus:

16.1. Patikslinama nustatytos susijusios informacinės sistemos ir įrenginiai bei sudaryta sąsajų schema, pateikiama UML 2, BPMN ar lygiaverčiu formatu;

16.2. serviso konfigūracijos patikrinimas (darbinės direktorijos pakeitimas, serviso teisių eskalavimas, informacijos atskleidimas per klaidų pranešimus ir pan.);

16.3. tikrinama, ar visų tipų informacinės sistemos naudotojai negali plėsti savo teisių sistemoje, atlikti veiksmų ir/arba gauti duomenų, nesusijusių su jų tiesioginių pareigų vykdymu;

16.4. tikrinamas DBVS atnaujinimo lygis ir konfigūracijos saugumas (laisva prieiga, per didelės naudotojų ar programų teisės, galimybė vykdyti sistemines komandas iš DBVS);

16.5. pažeidžiamumų paieška (naudotojo autentifikavimo mechanizmo patikrinimas, sesijos vientisumo patikrinimas, įvedamos informacijos apdorojimo patikrinimas, programinio kodo integralumo patikrinimas, klaidų pranešimų apdorojimas, sisteminės informacijos atskleidimas, serviso konfigūravimo klaidos) ne mažiau kaip trimis populiariausiais automatizuotais žiniatinklio pažeidžiamumo skeneriais;

16.6. Turi būti atliktas rankinis patikrinimas, ar identifikuoti pažeidžiamumai gali būti pritaikyti realiai (pašalinti false-positive);

16.7. pažeidžiamumų patikrinimas ne mažiau kaip pagal OWASP Application Security Verification Standard 3.0 antro lygio reikalavimus (ASVS Level 2), suderintus „OWASP Testing Guide v4“ metodikos punktus (neapsiribojant „OWASP Top 10“ pažeidžiamumais).

17. Turi būti atlikti vidinis ir išorinis sistemos kritinės apkrovos testai. Sistema tikrinama generuojant užklausas iš vienos, nustatytų techninių parametrų tarnybinės stoties ir stebimas atsakymo laikas. Testo tikslas įvertinti tolygiai didinamo užklausų kiekio poveikį sistemos greitaveikai, nesukeliant sistemos darbingumo sutrikdymo. Testavimas turi būti atliekamas iš anksto suderintu laiku.

18. Turi būti atlikta saugos sistemų įvykių žurnalų įrašų analizė, tikrinant ar šių įrašų pakanka vidinio ir išorinio įsibrovimo bandymams užfiksuoti, įsibrovėliui ir jo panaudotiems įsibrovimo metodams identifikuoti bei įvykiams atkurti. Tikrinama, ar įrašų saugojimo laikas atitinka minimalų informacinei sistemai reikalaujamą įrašų saugojimo laiką.

IV. DUOMENŲ TEIKIMUI NAUDOJAMŲ TECHNOLOGIJŲ SAUGUMO VERTINIMAS

19. Turi būti išanalizuotos ir ištestuotos technologijos, naudojamos duomenų teikimui automatiniu būdu pagal duomenų teikimo sutartis:

19.1. technologinis duomenų teikimo priemonių ir būdų pažeidžiamumų patikrinimas;

19.2. duomenų apsaugos algoritmų vertinimas, identifikuojant, ar nėra galimybės panaudoti nepakankamai saugius algoritmus ar šifravimo, autentifikavimo raktų ilgius;

19.3. tipinių įsilaužimo veiksmų, naudojamų informacijos perėmimui, atlikimas;

19.4. patikrinimas, ar sutarčių šalys negali eskaluoti savo teisių ar pasiekti daugiau informacijos nei joms priklauso pagal susitarimus.

20. Turi būti pateiktos ekspertinės saugumo konsultantų išvados ir rekomendacijos saugiam technologiniam duomenų teikimui.

21. Bendraujant su atsakingais darbuotojais, remiantis testavimo metu surinkta informacija, geriausiąja praktika ir standartais, įvertinamas vidinio duomenų perdavimo tinklo saugumas.

V. INFORMACINĖS SISTEMOS SAUGOS REIKALAVIMŲ ATITIKTIES VERTINIMO ATASKAITOS PARENGIMAS

22. Turi būti parengta detali technologinių pažeidžiamumų ataskaita techniniams specialistams, kurioje aprašyta:

22.1. tikrinti objektai ir tikrinimo tikslai;

22.2. testavimo eiga;

22.3. visos atakos ir visi saugumo testai, kurie buvo atlikti pagal paslaugos teikėjo naudojamą įsilaužimų testavimo metodologiją;

22.4. testo numeris ir pavadinimas;

22.5. testo/atakos paskirtis, atakos metrikos ir vektoriai, siekiamas tikslas ir trumpas aprašymas;

22.6. testo objektai, taikiniai (IP adresai, prievadų numeriai, atakuoti URL parametrai, atakuotų žiniatinklio formų parametrai ir kt.);

22.7. testui/atakai naudoti programiniai/aparatiniai įrankiai ir priemonės;

22.8. testo/atakos turinys, parašas, naudoto kenksmingo programinio kodo išeities tekstas, žiniatinklio užklausų parametrų reikšmės ir kt.;

22.9. testo ar testavimo įrankio išdavos (angl. *output*) ir pažeidžiamumo buvimo/nebuvimo įrodymai;

22.10. nustačius pažeidžiamumą, jis turi būti klasifikuotas pateikiant nuorodas į ITU-T X.1520 (04/2011) standarto reikalavimus atitinkančią pažeidžiamumų duomenų bazę (CVE ar lygiavertę) arba klasifikuotas pagal CVSS v3.0 ar lygiavertę metodiką;

22.11. testo rezultatai (sėkmė/nesėkmė, rankinio patikrinimo rezultatai), išvados, pažeidžiamumo pašalinimo rekomendacijos, šalinimo planas (suderintas su Klientu).

23. Pateikiami visi galimi įsilaužimų scenarijai – detaliai aprašyta veiksmų seka, kaip išnaudoti vieną ar kitą saugumo trūkumą (pateikiami tik esant technologiniams pažeidžiamumams).

24. Ataskaita turi leisti iš karto identifikuoti labiausiai pažeidžiamas VUSIS vietas ir didžiausius trūkumus, o atlikus pakartotinius pažeidžiamumų įvertinimus ateityje, leisti palyginti gautus rezultatus ir įvertinti pokyčius.

25. Identifikuoti pažeidžiamumai turi būti sugrupuoti pagal kritiškumą (angl. Severity), panaudojant kokybinio ir kiekybinio vertinimo skales (CVSS v3.0 Severity Rating Scale ar lygiavertes).

26. Turi būti parengtos išvados ir informacijos sistemos saugos reikalavimų atitikties vertinimą apibendrinanti suvestinė ataskaita. Šioje ataskaitoje turi atsispindėti statistika, tendencijos, bendra saugumo būklė, pavojingiausi pažeidžiamumai, saugumo trūkumai ir prioretizuotos saugumo gerinimo kryptys. Remiantis testavimo metu surinkta informacija, geriausiąja praktika ir standartais, įvertinamas duomenų perdavimo tinklo saugumas ir pateikiamos rekomendacijos.

27. Kompaktiniame diske turi būti pateikti skenavimo/testavimo priemonių ir testų rezultatai.

KLIENTAS
Vilniaus universitetas,

Kancleris Gediminas Miškinis

(parašas) A. V.

PASLAUGŲ TEIKĖJAS
UAB „IO projects“

Direktorius Ignas Griškevičius

(parašas) A. V.

VU Viešųjų pirkimų direkcijos
vyresnysis specialistas
Karolis Urbanavičius

Sutarties priedas Nr. 2

2016-11-04
Nr. APS-520000-1526

SPECIALISTŲ SĄRAŠAS

1. Projekto vadovas:

Eil. Nr.	Vardas, pavardė	Turimi kvalifikacijos egzaminų sertifikatai
1.	Ignas Griškevičius	Comptia Project+

2. Informacijos saugos valdymo sistemų auditorius:

Eil. Nr.	Vardas, pavardė	Turimi kvalifikacijos egzaminų sertifikatai
1.	Žydrūnas Skardžius	Certified Information system Auditor

3. Informacinių sistemų technologinio pažeidžiamumo patikrinimo specialistas (ekspertas):

Eil. Nr.	Vardas, pavardė	Turimi kvalifikacijos egzaminų sertifikatai
1.	Viktoras Monkevičius	Licenced penetration tester

4. Informacinių sistemų įsilaužimų metodikų pritaikymo specialistas (ekspertas):

Eil. Nr.	Vardas, pavardė	Turimi kvalifikacijos egzaminų sertifikatai
1.	Viktoras Monkevičius	Certified ethical hacker

KLIENTAS
Vilniaus universitetas,

Kancleris Gediminas Miškinis

(parašas) A. V.

PASLAUGŲ TEIKĖJAS
UAB „IO projects“

Direktorius Ignas Griškevičius

(parašas) A. V.

VU Viešųjų pirkimų direkcijos
vyresnysis specialistas
Karolis Urbanavičius

Sutarties priedas Nr. 3

PASLAUGŲ PERDAVIMO – PRIĖMIMO AKTAS

Vilnius, 2016- -

Atsižvelgiant į tai, kad 201 m. _____ d. tarp [***Pavadinimas***] ir Vilniaus universiteto buvo pasirašyta sutartis Nr. _____, dėl xxxxxxx paslaugų pirkimo, [***Pavadinimas***], kurios adresas yra [***adresas***], tinkamai [***suteikė/nesuteikė***], o Vilniaus universitetas, registruotas adresu Universiteto g. 3, LT-01513 Vilnius, atstovaujamas [*pareigos, vardas, pavardė*], veikiančio pagal [*atstovavimo pagrindas*], [***priėmė/nepriėmė***] paslaugas pagal 201 m. _____ mėn. __ d. Paslaugų pirkimo-pardavimo sutartį Nr. _____.

KLIENTAS
Vilniaus universitetas,
Įmonės kodas 211950810,
PVM mokėtojo kodas LT119508113,
Adresas: Universiteto 3, Vilnius, LT-01513
A/s LT537300010002460768
AB „Swedbank“
Banko kodas 73000

[***Vardas, Pavardė***]

_____
_____
(parašas)

PASLAUGŲ TEIKĖJAS
[***Pavadinimas***]
Įmonės kodas: xxxxxxxxx
PVM mokėtojo kodas: xxxxx
Adresas: xxxxxxxxx
A/s: xxxxxxxxx
Bankas: xxxxxxxxxxxxxxx
Banko kodas: xxxxxxxxx

[***Vardas, Pavardė***]

_____
_____
(parašas)