APLINKOS INFORMACIJOS VALDYMO INTEGRUOTOS KOMPIUTERINĖS SISTEMOS ĮSILAUŽIMŲ TESTAVIMO PASLAUGŲ
TECHNINĖ SPECIFIKACIJA

Terminai ir sutrumpinimai

Terminai / sutrumpinimai	**Paaiškinimas**
AIVIKS	Aplinkos informacijos valdymo integruota kompiuterinė sistema
ALIS	Aplinkosauginių leidimų informacinė sistema
API	Aplikacijų programavimo sąsaja (angl. Application programming interface; sistema – sistemai)
DBSIS	Dokumentų valdymo bendrosios informacinės sistemos
eIDAS	Elektroninio identifikavimo, autentifikavimo ir patikimumo užtikrinimo paslauga (2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB)
ES	Europos sąjunga
F-dujų	Fluorintos šiltnamio efektą sukeliančios dujos ir ozono sluoksnį ardančios medžiagos
GR	Gyventojų registras
IMAS	Išmanioji mokesčių administravimo sistema
IP	Išorinis portalas
JAR	Juridinių asmenų registras
LAND-43	Kurą deginančių įrenginių norma LAND-43 2013
LIMS	Laboratorinės informacijos valdymo sistema
LOJ	Lakieji organiniai junginiai
NTIS	Nuotekų tvarkymo informacinė sistema
OKTIS	Oro kokybės tyrimų informacinė sistema
PožVIS	Požeminio vandens informacinė sistema
RC	Valstybės įmonė Registrų centras
TPPIS	Taršos prevencijos procesų informacinė sistema
UETK	Lietuvos Respublikos upių, ežerų ir tvenkinių kadastras
ŪS	Ūkio subjektas (fizinis, juridinis asmuo, organizacija ar jų padaliniai)
VDV IS	Valstybės duomenų valdysenos informacinė sistema
VIISP	Elektroninių valdžios vartų „Valstybės informacinių išteklių sąveikumo platforma“ „Administracinių ir viešųjų elektroninių paslaugų portalas“
VMI	Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos
VP	Vidinis portalas

1. BENDRA INFORMACIJA APIE PROJEKTĄ IR PIRKIMĄ

1.1. Aplinkos apsaugos agentūra (toliau – Pirkėjas arba AAA), įgyvendindama projektą ,,Aplinkos informacijos valdymo integruotos kompiuterinės sistemos (AIVIKS) modernizavimas“ Nr. 01-010-P-0001 (toliau – Projektas), kuris finansuojamas pagal 2021–2027 metų Europos Sąjungos fondų investicijų programoje numatytas investicijas: „atnaujinti Aplinkos informacijos valdymo integruotą kompiuterinę sistemą (AIVIKS), siekiant sukurti progresyvią informacinę sistemą, užtikrinančią sąsajas su kitomis informacinėmis sistemomis, tobulinti duomenų surinkimo, sisteminimo, kaupimo, analizės ir publikavimo procesus“, Sanglaudos fondo ir valstybės biudžeto lėšomis, perka AIVIKS įsilaužimų testavimo paslaugas. Projekto tikslas - efektyvinti, modernizuoti, plėsti esamą AIVIKS, darant ją patogesnę, išsamesnę ir patrauklesnę naudotojams. AIVIKS naudotojai (fiziniai, juridiniai asmenys). Suinteresuotos Projekto šalys – Aplinkos ministerija, Aplinkos apsaugos agentūra ir Aplinkos apsaugos departamentas prie Aplinkos ministerijos, Aplinkos projektų valdymo agentūra.

1.2. Pirkimo tikslas – siekiant Projekto tikslo yra perkamos įsilaužimo testavimo paslaugos - informacinės saugos bei duomenų perdavimo tinklo infrastruktūros ir informacinių sistemų saugumo audito ir įsilaužimo testo paslaugos (toliau – Paslaugos), kurių reikalavimai yra išvardinti šioje techninėje specifikacijoje.

1.3. Pirkimo ir sutarties vykdymui aktualūs teisės aktai

Eil. Nr.	**Teisės aktas**
1.	Lietuvos Respublikos kibernetinio saugumo įstatymas;
2.	Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;
3.	Lietuvos Respublikos Valstybės informacinių išteklių valdymo įstatymas
4.	Lietuvos Respublikos viešųjų pirkimų įstatymas;
5.	2016 m. balandžio 27 d. Europos Parlamento ir Tarybos Reglamentu (ES) 2016/679 „Dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB“ (Bendrasis duomenų apsaugos reglamentas);
6.	Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, saugos dokumentų turinio gairių aprašo ir elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas);
7.	Informacinių sistemų steigimo, kūrimo, atnaujinimo, pertvarkymo ir likvidavimo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2024 m. gegužės 15 d. nutarimu Nr. 349 „Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo įgyvendinimo“;
8.	Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;
9.	Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų aprašu, patvirtintu 2020 m. lapkričio 26 d. Lietuvos Banko valdybos nutarimu Nr. 03-174 „Dėl Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų aprašo patvirtinimo“;
10.	Valstybinės duomenų apsaugos inspekcijos „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairių duomenų valdytojams ir duomenų tvarkytojams“ 2020 m. birželio mėn. 18 d. gairėmis https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2020-06-18.pdf;
11.	Lietuvos standartais LST EN ISO/IEC 27002 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“, LST EN ISO/IEC 27001 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/EC 27005 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo rizikos valdymas“ ir kiti standartai;
12.	Lietuvos Respublikos informacinių išteklių valdymo įstatymas;
13.	INFORMACINĖS SISTEMOS „APLINKOS INFORMACIJOS VALDYMO INTEGRUOTA KOMPIUTERINĖ SISTEMA“ (IS „AIVIKS“) NUOSTATAI

1.4. Tiekėjas (toliau – Tiekėjas) teikdamas Paslaugas turės užtikrinti, kad jo teikiamos Paslaugos pagal Lietuvos Respublikos viešųjų pirkimų įstatymo 37 str. 9 d. 2 p. nekeltų grėsmės nacionaliniam saugumui. Taip pat teikdamas Paslaugas privalės laikytis teisės aktų reikalavimų, nustatančių duomenų apsaugą bei teikti Paslaugas taip, kad visi su teikiamomis Paslaugomis susiję veiksmai atitiktų BDAR.

1.5. Paslaugų teikimo etapai:

Etapo Nr.	Etapo pavadinimas	Etapo aprašymas
1.	Pirminis atsparumo vertinimas ir įsilaužimų testavimas	AIVIKS modernizuotų funkcionalumų pirminis vertinimas ir įsilaužimų testavimas
2.	Tarpinis įsilaužimų testavimas	AIVIKS modernizuotų funkcionalumų tarpinis vertinimas ir įsilaužimų testavimas
3.	Galutinis atsparumo vertinimas ir įsilaužimų testavimas	AIVIKS modernizuotų funkcionalumų galutinis vertinimas ir įsilaužimų testavimas

1.6. Tiekėjas teikia Paslaugas naudodamas Pirkėjo IT infrastruktūrą;

1.7. Tiekėjas turės suteikti Paslaugas, išvardintas šioje techninėje specifikacijoje. Apibūdinant pirkimo objektą, techninėje specifikacijoje ar kituose pirkimo dokumentuose galimai nurodytas konkretus modelis ar tiekimo šaltinis, konkretus procesas, būdingas konkretaus tiekėjo tiekiamoms prekėms ar teikiamoms paslaugoms, ar prekių ženklas, patentas, tipai, konkreti kilmė ar gamyba, sertifikatai, standartai, protokolai turi būti suprantami su žodžiais „arba lygiavertis“.

1.8. Tiekėjas Paslaugas turės teikti nuotoliniu būdu, visi susitikimai organizuojami nuotoliniu būdu ir tik pagal poreikį gyvai. Paslaugoms teikti nenaudojami popieriniai dokumentai, techninė dokumentacija, Paslaugų užsakymai, Paslaugų priėmimo-perdavimo aktai ir kiti dokumentai teikiami tik elektroninėje formoje.

1.9. Paslaugų teikimo laikas – Pirkėjo darbo dienomis nuo 08:00 iki 17:00 val., penktadieniais nuo 08:00 iki 15:45 val., darbo dienos trukmė prieš šventines dienas – viena valanda trumpiau (UTC + 02:00, pasaulinis koordinuotasis laikas). Pirkėjo ir Tiekėjo susitarimu Paslaugos gali būti teikiamos ne Pirkėjo darbo valandomis.

1.10. Tiekėjas Paslaugas teiks pagal Pirkėjo pateiktą konkrečią užduotį.

1.11. Tiekėjas įsipareigoja vykdant esamų AIVIKS funkcionalumų įsilaužimų testavimą naudoti iteracinį metodą Agile Scrum, Pirkėjo įgyvendintoje „Atlassian“ programinės įrangos „Jira“ priemonėmis (JIRA Atlassian).

2. ESAMOS PADĖTIES APRAŠYMAS

Augantys visuomenės poreikiai viešojo sektoriaus institucijose kaupiamų duomenų ir informacijos bei elektroninių paslaugų prieinamumui bei naudojimo patogumui kelia naujus uždavinius ir tikslus Pirkėjo tvarkomai AIVIKS informacinei sistemai, kuri turi būti orientuota į vartotoją, patogi naudoti, teikti sąveikias ir pažangias elektronines paslaugas bei užtikrinti jų prieinamumą. Atsižvelgdamas į šiandienos realijas, Pirkėjas siekia identifikuoti esamų paslaugų vystymo bei naujų paslaugų sukūrimo galimybes AIVIKS informacinėje sistemoje.

AIVIKS sistema buvo pradėta eksploatuoti 2013 m. Ši sistema suteikia fiziniams ir juridiniams asmenims galimybes gauti išsamią informaciją apie aplinkos būklę, teikti teisės aktų nustatyta tvarka aplinkosaugines ataskaitas elektroninėje formoje. Pagrindinės AIVIKS funkcijos yra:

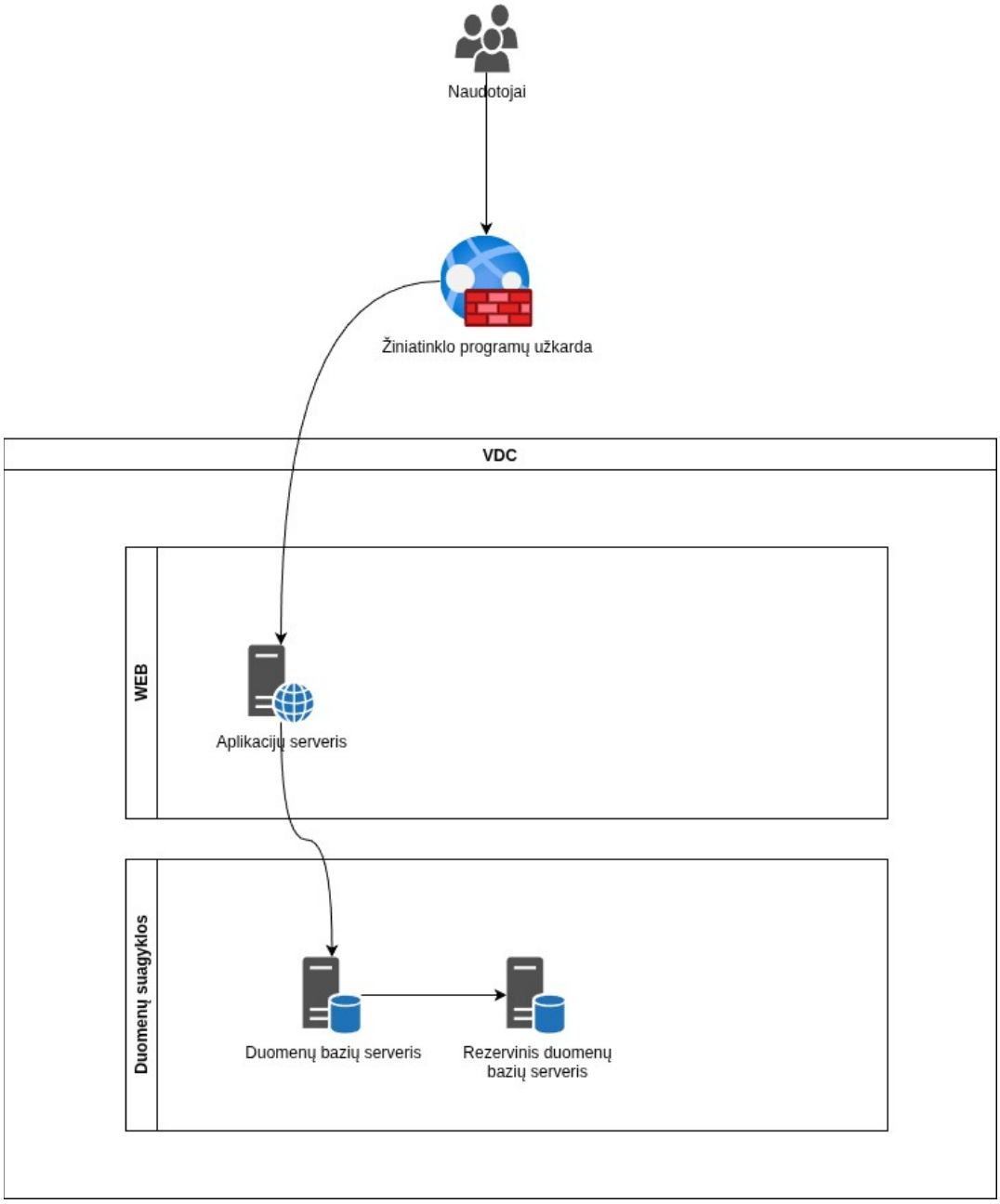
Palengvinti Pirkėjo ir Lietuvos Respublikos aplinkos ministerijai pavaldžių institucijų darbuotojų ir tarnautojų darbą / veiklą kaupiant, sisteminant, analizuojant, naudojant ir teikiant aplinkos duomenis bei informaciją.

Teikti elektronines paslaugas fiziniams ir juridiniams asmenims suteikiant jiems galimybę teikti teisės aktų reikalavimais nustatytas aplinkosaugines ataskaitas.

Užtikrinti informacijos apie aplinką prieinamumą fiziniams ir juridiniams asmenims, visuomenei bei Lietuvos Respublikos, Europos Sąjungos ir tarptautinėms institucijoms.

2.1. ESAMA AIVIKS TECHNINĖ ARCHITEKTŪRA

Architektūroje išskiriamos pagrindinės viešųjų ir vidinių paslaugų sritys. Dėl naudotojų darbo su sistema specifikos šios sritys yra logiškai atskirtos. Žemiau (pav. 1) pateikiama detalizuota sistemos loginė techninė architektūra, detalesnė informacija yra pateikta lentelėse Nr. 1, Nr. 2, Nr. 3, Nr. 4, Nr. 5.



Pav. 1 Sistemos loginė techninė architektūra

Eksploatuojama techninė įranga

1 lentelė. Tarnybinių stočių, toliau vadinamų serveriais, programinė įranga

Eil. Nr.	Paskirtis	Programinės įrangos pavadinimas
1.	Aplikacijų serveris	PHP 8.4
2.	Duomenų bazių valdymo serveris	MariaDB 10.11

2 lentelė. Serverių kiekiai

Eil. Nr.	Komponentas	Vnt.
1.	Aplikacijų serveris	1
2.	Duomenų bazių valdymo serveris	1
3.	Žiniatinklio programų užkarda (WAF)	1

3 lentelė. Aplikacijų serverio techniniai parametrai

Eil. Nr.	Charakteristikos pavadinimas	Parametro reikšmė
1.	Procesoriaus parametrai	2 vnt., 2.9GHz, 8 branduolių
2.	Operatyvinė atmintis	32 GB
3.	Vidinis kietasis diskas	130 GB
4.	Operacinė sistema	Ubuntu server 24.04 LTS
5.	Paskirtis	Programų serveris – PHP 8.4

4 lentelė. Duomenų bazės serverio techniniai parametrai

Eil. Nr.	Charakteristikos pavadinimas	Parametro reikšmė
1.	Procesoriaus parametrai	2 vnt., 2.9GHz, 8 branduolių
2.	Operatyvinė atmintis	32 GB
3.	Vidinis kietasis diskas	130 GB su praplėtimu
4.	Operacinė sistema	Ubuntu server 24.04 LTS
5.	Paskirtis	Duomenų bazės serveris – MariaDB 10.11

Naudojamos išorinės paslaugos:

- Žiniatinklio programų užkarda (WAF) paslauga
- F5 Advanced WAF pagrindu veikianti WAF ir DDoS apsauga

Programinė įranga

5 lentelė. Esama programinė įranga

Eil. Nr.	Komponentas	Licencijų kiekis	Licencijos tipas
1.	Ubuntu server 24.04 LTS	2	Nemokama
2.	PHP 8.4	1	Nemokama
3.	MariaDB 10.11	1	Nemokama

2.2. AIVIKS ARCHITEKTŪRA

2.2.1 Pagal apibendrintą AIVIKS funkcionalumą išskirtos šios atskiros sistemos:

• duomenų teikimo sistema – ūkio subjektams skirta sistema, kurioje gali teikti ataskaitas;

• duomenų tvarkymo sistema – vidiniams naudotojams skirta sistema, kuriai padedant tvarkomi AIVIKS duomenys. Realizuotos duomenų tvarkymo formos apima dalykinius ir bendruosius duomenis;

• administravimo sistema – sistemos administratoriams skirta sistema, kurioje gali atlikti AIVIKS sistemos administravimo veiklas, klasifikacinių duomenų tvarkymą ir pan.

Išvardintos sistemos įgyvendina specifinėms veiklos sritims - posistemiams reikalingą funkcionalumą, diferencijuotą pagal šias veiklas vykdančias organizacijas ir padalinius.

2.2.2 AIVIKS sudaro šie posistemiai:

01. Išmetamų teršalų iš kurą deginančių įrenginių (LAND) posistemis;
02. Lakiųjų organinių junginių (LOJ) posistemis;

03. Duomenų apie fluorintas šiltnamio efektą sukeliančias dujas (F-dujų) posistemis;
04. Administravimo posistemis;
05. Cheminių medžiagų ir mišinių posistemis;
06. Oro ataskaitos posistemis;
07. Oro taršos inventorizacijos posistemis;
08. Stacionarių taršos šaltinių mokesčių posistemis.
Šiuo metu AIVIKS yra modernizuojama todėl posistemių sąrašas nėra baigtinis.

2.3. AIVIKS NAUDOJAMOS INTEGRACIJOS

- Valstybės įmonė Registrų centras - teikia Juridinių asmenų ir adresų registrų duomenis;
- Lietuvos Respublikos aplinkos ministerija - teikia Lietuvos Respublikos upių, ežerų ir tvenkinių kadastro duomenis;
- Lietuvos geologijos tarnyba prie Aplinkos ministerijos – teikia Žemės gelmių registro ir Valstybinės požeminio vandens informacinės sistemos duomenis;
- Nacionalinė žemės tarnyba prie Aplinkos ministerijos – teikia Georeferencinio pagrindo duomenis;
- Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos - teikia VIISP duomenis;
- Valstybinė duomenų agentūra – Ekonominės veiklos rūšių klasifikatorius;
- Lietuvos Respublikos aplinkos ministerija - teikia Aplinkosaugos leidimų informacinės sistemos duomenis.

3. REIKALAVIMAI PASLAUGOMS

3.1. Bendrieji reikalavimai. Informacinės saugos bei duomenų perdavimo tinklo infrastruktūros ir informacinių sistemų saugumo audito ir įsilaužimo testo paslaugos:

3.1.1. išorinio kompiuterinio tinklo perimetro patikrinimo (testavimo) paslaugos: išorinio kompiuterinio tinklo perimetro patikrinimas (patikrinimas atliekamas turint minimalias žinias apie tikrinamos organizacijos IT (Informacinių technologijų) infrastruktūrą imituojant potencialaus įsilaužėlio iš interneto veiksmus):

3.1.1.1. perimetro tinklo mazgų, pasiekiamų iš interneto nustatymas;

3.1.1.2. perimetro tinklo mazguose veikiančių OS (Operacinių Sistemų) nustatymas ir atitinkamų, pažeidžiamumų patikrinimas;

3.1.1.3. perimetro tinklo mazguose veikiančių tarnybų nustatymas ir atitinkamų, pažeidžiamumų patikrinimas, bei konfigūracijos analizė (papildomos informacijos apie sistemą surinkimas per klaidų, sisteminius pranešimus, servisų programinę realizaciją);

3.1.1.4. nustačius pažeidžiamumus atliekamas įsilaužimo testas;

3.1.1.5. jei aptinkama iš interneto pasiekiamų tarnybų, reikalaujančių vartotojo autentifikacijos, tuomet atliekamas išorinės paslaugos slaptažodžių auditas. Tikrinama ar naudojami patikimi slaptažodžiai, ar įmanoma juos atspėti arba parinkti.

3.1.2. vidinio tinklo (LAN) infrastruktūros saugos patikrinimas (testavimas):

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

3.1.2.2. patikrinamas tarnybinių stočių operacinės sistemos ir jose veikiančios sisteminės programinės įrangos atnaujinimo lygis ir ar jos nėra pažeidžiamos remiantis saugumo spragomis;

3.1.2.3. patikrinamas tarnybinių stočių ir jose veikiančios sisteminės programinės įrangos konfigūracijos saugumas;

3.1.2.4. patikrinamas prisijungimo prie Tarnybinių stočių saugumas, naudojant anoniminį / nesankcionuotą prisijungimą ir / arba turint eilinio vartotojo prisijungimo duomenis;

3.1.2.5. patikrinama ar vartotojai negali eskaluoti savo teisų sistemoje, atlikti veiksmus ir/arba gauti duomenis, nesusijusius su jų tiesioginių pareigų vykdymu;

3.1.2.6. vidinio duomenų perdavimo tinklo saugumo tikrinimas, remiantis surinkta informacija, patikrinimo metu nustatyta realia padėtimi, geriausiąja praktika ir standartais;

3.1.2.7. perduodamų / priimamų duomenų perėmimo galimybės ir manipuliavimas jais.

3.1.2.8. kiti testai pagal Tiekėjo naudojamą metodologiją;

3.1.3. vidinių informacinių sistemų, veikiančių WEB aplikacijų pagrindu, patikrinimas, API paslaugų patikrinimas:

3.1.3.1. WEB aplikacijų testavimas, įsilaužimų testai;

3.1.3.2. WEB aplikacijų taikomųjų programų ir paslaugų saugumo patikrinimas neturint naudotojo prisijungimo informacijos;

3.1.3.3. informacijos apie sistemas surinkimas (informacija apie sistemą, periferines / pagalbines sistemas) ir testavimo ribų nustatymas;

3.1.3.4. tinklo mazguose veikiančių tarnybų nustatymas ir atitinkamų pažeidžiamumų patikrinimas, bei konfigūracijos analizė (papildomos informacijos apie sistemą surinkimas per klaidų, sisteminius pranešimus, tarnybų programinę realizaciją);

3.1.3.5. naudojamų technologijų identifikavimas (platforma, programavimo metodai ir priemonės);

3.1.3.6. tarnybų konfigūracijos patikrinimas (darbinės direktorijos pakeitimas, serviso teisių eskalavimas, informacijos atskleidimas per klaidų pranešimus);

3.1.3.7. pažeidžiamumų paieška (vartotojo autentifikavimo mechanizmo patikrinimas, sesijos vientisumo patikrinimas, įvedamos informacijos apdorojimo patikrinimas, programinio kodo integralumo patikrinimas, klaidų pranešimų apdorojimas, sisteminės informacijos atskleidimas, serviso konfigūravimo klaidos) automatizuotais WEB pažeidžiamumo skeneriais;

3.1.3.8. automatizuotos paieškos rezultatų patikrinimas, klaidingų suveikimų pašalinimas.

3.1.4. Programinės įrangos vystymo ir diegimo sistemų auditas:

3.1.4.1. GIT platformos konfigūracijos auditas;

3.1.4.2. nuolatinio vystymo ir integravimo sistemų auditas (CI/CD).

3.1.5. Paslaugų etapas Nr. 2 gali būti atliekamas pasitelkiant automatinius įsilaužimų testavimo įrankius ir gali būti skaidomas dalimis. Automatizuoti testai atlikti pripažintais saugumo skeneriais (OWASP rekomenduotais įrankiais).

3.2. Specialieji reikalavimai Paslaugoms

Nr.	Reikalavimas
1.	Pateiktų WEB svetainių spragų patikrinimas pagal šiuos kriterijus: - OWASP Top 10 and beyond, naudojantis OWASP WSTG metodologija; - autentifikacijos mechanizmų testavimas (MFA / SSO); - API tarnybų testavimas; - automatizuotos paieškos rezultatų patikrinimas, klaidingų suveikimų pašalinimas; - rankinis testavimas, ypatingą dėmesį skiriant OWASP TOP 10 pažeidžiamumams.
2.	Parengti atsparumo įsilaužimams testavimo metodiką. Iki testavimo pradžios parengti ir susiderinti veiksmų gairių/ taisyklių (rules of engagement (ROE)) dokumentą. Teikiant Paslaugas vadovautis naujausia saugaus projektavimo ir kodavimo praktika ir metodais saugumo patikrinimo metodikomis, siekiant užtikrinti, kad Paslaugų rezultatai neturėtų saugumo spragų.
3.	Naudojami vertinimo kriterijai turi būti objektyvūs, išsamūs, tinkami vertinamam objektui, išmatuojami, suprantami, plačiai pripažinti, autoritetingi ir suprantami Pirkėjui. Turi būti žinomi atitikties kriterijų pasirinkimo šaltiniai, o patys kriterijai suderinti su Pirkėju. Taip pat Tiekėjas turės suderinti su Pirkėju Paslaugų teikimo metu naudojamus vertinimo būdus, metodus ir priemones prieš pradedant IS saugumo auditą.
4.	Naudojami pažeidžiamumo identifikavimo, įsilaužimo testavimo (kibernetinių atakų imitavimo) metodai turi būti naudojami ir kontroliuojami taip, kad nebūtų sukeltas neigiamas poveikis testuojamiems objektams (pvz., sistemų ir su jomis susijusių sistemų duomenų sugadinimas, veiklos sutrikdymas, apsaugos išjungimas arba apsaugos sumažinimas ir pan.) arba prieš testavimą turi būti imamasi visų įmanomų priemonių (pvz., atsarginės kopijos ir kt.), kad būtų operatyviai pašalinti visi neigiami testavimo padariniai. Jeigu dėl Tiekėjo vykdomų veiksmų įvyks įrangos, sistemos gedimas ar duomenų vientisumo pažeidimas ar praradimas, įrangos, sistemos funkcionalumas ar (ir) duomenys turi būti atstatomi Tiekėjo finansiniais ir kitokiais ištekliais ne vėliau kaip per 8 val. nuo incidento (įrangos gedimo, duomenų vientisumo pažeidimo ar praradimo) užfiksavimo momento.
5.	Saityno paslaugų taikomųjų programų vertinimo metu turi būti atlikta: - automatizuotas arba rankinis patikrinimas turi būti atliekamas pagal visus punktus nurodytus https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/ . - Po automatizuotos patikros turi būti atliktas rezultatų rankinis patikrinimas su tikslu įvertinti realią pažeidžiamumo galimybę ir grėsmę. - pažeidžiamumų paieškai privalu naudoti pažeidžiamumo skeneriais nurodytais https://owasp.org/www-project-web-security-testing-guide/v42/6-Appendix/A-Testing_Tools_Resource - atliktas IS kritinės apkrovos testas. IS tikrinama generuojant užklausas iš bent dešimties

Nr.	Reikalavimas
	(10), nustatytų techninių parametrų tarnybinių stočių ir stebimas atsakymo laikas. Testo tikslas įvertinti tolygiai didinamo užklausų kiekio poveikį IS greitaveikai, nesukeliant IS darbingumo sutrikdymo. - saugos sistemų įvykių žurnalų įrašų analizė, tikrinant ar šių įrašų pakanka įsibrovimo bandymams užfiksuoti, įsibrovėliui ir jo panaudotiems įsibrovimo metodams identifikuoti bei įvykiams atkurti. Tikrinama, ar įrašų saugojimo laikas atitinka minimalų IS reikalaujamą įrašų saugojimo laiką.
6.	Saityno paslaugų taikomųjų programų išeities (programinio) kodo ir pažeidžiamumo vertinimo metu turi būti atliekama: - išeities kodo ir API (aplikacijų programavimo sąsajų) analizė automatiniu ir rankiniu būdu. API saugumo testavimas turi būti atliktas siekiant nustatyti galimus pažeidžiamumus tarp skirtingų IS integracijų (įvertinti sistemos integracijų modulius); - patikrinami rankiniu ir automatiniu būdu programinio išeities kodo pažeidžiamumai (asmens duomenys pateikiami atviru tekstu, autentifikavimo, prieigos prie objektų problemos, nesaugus šifravimas ir kt. testai pagal tiekėjo siūloma metodologiją), kartu testuojant ir veikiančią programinę įrangą (dinaminis testavimas). Rankiniu būdu turi būti tikrinama tik ta IS programinio kodo ir API dalis, kuri tiesiogiai dalyvauja perduodant ir tvarkant asmens duomenis; - testavimo priemonės turi palaikyti technologijas naudojamas Pirkėjo aplinkoje (įskaitant, bet neapsiribojant): PHP, HTML, CSS, nginx, JavaScript, TypeScript; - naudojamos priemonės turi būti pritaikytos aptikti ir identifikuoti šio tipo pažeidžiamumus išeities kode: CrossSite Scripting, Injection, BufferOverflow, Path Traversal, Denial of Service, Validation; - naudojama priemonė turi būti pritaikyta identifikuoti pažeidžiamumus.
7.	Duomenų teikimui naudojamų technologijų saugumo vertinimo metu turi būti atliekama: Turi būti išanalizuoti ir ištestuoti visi būdai, naudojami duomenų teikimui automatiniu būdu pagal duomenų teikimo sutartis: - technologinis duomenų teikimo priemonių ir būdų pažeidžiamumų patikrinimas; - duomenų apsaugos algoritmų vertinimas, identifikuojant ar nėra galimybės panaudoti nepakankamai saugius algoritmus ar šifravimo, autentifikavimo raktų ilgius; - tipinių įsilaužimo veiksmų, naudojamų informacijos perėmimui, atlikimas; - patikrinimas, ar sutarčių šalys negali eskaluoti savo teisių ar pasiekti daugiau informacijos nei joms priklauso pagal susitarimus. - turi būti pateiktos ekspertinės saugumo konsultantų išvados ir rekomendacijos saugiam technologiniam duomenų teikimui.
8.	IS duomenų bazių valdymo sistemos patikrinimas: - tikrinamas DBVS atnaujinimo lygis ir konfigūracijos saugumas (laisva prieiga, per didelės naudotojų ar programų teisės, galimybė vykdyti sistemines komandas iš DBVS); - tikrinama, ar naudotojai negali eskaluoti savo teisų IS, atlikti veiksmus ir/arba gauti duomenis, nesusijusius su jų tiesioginių pareigų vykdymu; - tikrinama, ar darbuotojams ir IS ar paslaugoms suteikta prieiga prie DBVS atitinka mažiausios privilegijos principą. Šis principas reiškia, kad turi būti suteikiamos tik minimalios darbuotojų, IS ar paslaugų tiesioginei veiklai vykdyti reikalingos prieigos teisės bei organizacinėmis ir techninėmis priemonėmis užtikrinama minimalių prieigos teisių naudojimo kontrolė (pvz., privilegijuotos prieigos teisės neturi būti naudojamos veiklai, kuriai atlikti pakanka žemesnio lygio prieigos teisių, pvz., saityno paslaugoms teikti nenaudojamos root teisės, ir pan.).
9.	Turi būti parengta ir Pirkėjui pristatyta AIVIKS atsparumo įsilaužimui ataskaita, kurios turinys turi apimti šias sritis: 1. Tikrintų objektų aprašymas (nurodoma kokie AIVIKS testavimai atlikti); 2. Patikrinimo tikslai, eiga, metodai ir identifikuotos problemos;
10.	Rezultatai: 1. aprašomos aptiktos spragos, pateikiami įrodymai ir šalinimo rekomendacijos; 2. pateikiami įsilaužimo scenarijai – detaliai aprašoma veiksmų seka, kaip išnaudoti vieną ar kitą saugumo trūkumą (pateikiami tik esant technologiniam pažeidžiamumui);

Nr.	Reikalavimas
	3. pateikiami siūlymai, kaip pašalinti pažeidžiamumus; 4. kiekvienam aptiktam pažeidžiamumui ar saugumo trūkumui, pagal poveikį ir pasireiškimo tikimybę priskiriami rizikos įverčiai (žema, vidutinė, aukšta, kritinė), bei pateikiama metodika, pagal kurią šie įverčiai priskiriami; 5. Pateikiamos išvados;
11.	AIVIKS programavimo paslaugų tiekėjams pašalinus nustatytus pažeidimus turi būti atliktas pakartotinis atsparumo įsilaužimams testavimas ir atnaujinta ataskaita pateikiant joje informaciją apie nustatytų saugos trūkumų likvidavimą. Ne vėliau kaip per 2 savaites nuo informavimo apie pašalintus trūkumus.

3.3. Reikalavimai dokumentacijai

Nr.	Reikalavimas
1.	Visa Tiekėjo rengiama dokumentacija turi būti parengta lietuvių kalba ir laikantis bendrinės lietuvių kalbos taisyklių.
2.	Paslaugų teikimo metu Tiekėjas prieš pradėdamas rengti paslaugų teikimo sutarties vykdymo rezultatus (dokumentus) preliminarų jų turinį ir formą turi suderinti su Pirkėju.
3.	Dokumentų galutinės versijos turi būti pateiktos dviem formatais: redagavimui tinkamu elektroniniu (.doc, .docx, .odt arba lygiaverčiu formatu) ir atsakingo už sutartį asmens parašu pasirašytu formatu.
4.	Testavimo ataskaitos minimalus turinys: - Aprašyti testuoti objektai, testavimo metodai ir eiga; - Detaliai aprašytos rastos spragos, jų poveikio lygis (rizikos įvertinimai) ir grėsmės lygis; - Pateikti konkretūs įsilaužimo scenarijai (jei nustatyti); - Pateiktos aiškios rekomendacijos spragų šalinimui; - Nurodyta naudota metodika ir testavimo įrankiai.
5.	Pirkėjui ar kitoms suinteresuotoms šalims pateikus pastabas vertinamai dokumentacijai, Tiekėjas turi atlikti pataisymus atsižvelgdamas į šiuos reikalavimus:
5.1.	Iki 50 psl. apimties dokumentai turi būti pataisomi ne ilgiau kaip per 5 d. d.;
5.2.	Iki 100 psl. apimties dokumentai turi būti pataisomi ne ilgiau kaip per 10 d. d.;
5.3.	Didesnių nei 100 psl. apimties dokumentai turi būti pataisomi pagal susitarimą su Pirkėju.

3.4. Paslaugų teikimo metu, atsiradus aplinkybėms, kurių nebuvo galima iš anksto numatyti, gali būti keičiami techninėje specifikacijoje nurodyti reikalavimai į analogiškos apimties (vertės) kitą ar kitus reikalavimus. Pakeitimas turi būti įforminamas tarp Pirkėjo ir Tiekėjo raštu, laikantis Viešųjų pirkimų įstatymo 89 straipsnio nuostatų.

4. REIKALAVIMAI PASLAUGŲ TEIKIMO VALDYMUI:

4.1. Tiekėjas turi paskirti iš savo pusės asmenį, kuris būtų atsakingas už:

4.1.1. Paslaugų teikimo koordinavimą ir ataskaitų teikimą;

4.1.2. rizikų stebėseną ir komunikaciją su Pirkėju ir kitomis su Projektu suinteresuotomis šalimis.

4.2. Tiekėjas turi užtikrinti, kad visa komunikacija Paslaugų teikimo metu vyktų lietuvių kalba. Jei Paslaugas teikiantys specialistai nemoka lietuvių kalbos, Tiekėjas turi pasirūpinti vertimo į lietuvių kalbą paslaugomis.

4.3. Įvykus susitikimams Paslaugų teikimo klausimais tarp Tiekėjo ir Pirkėjo ar kitų suinteresuotų šalių, Tiekėjas turi parengti ir pateikti susitikime dalyvavusioms šalims suderintus susitikimų protokolus, kuriuose turi būti aprašomi aptarti klausimai ir priimti sprendimai.

4.4. Pirkėjas suteiks elektroninį žurnalą, reikalingą registruoti incidentus per internetinę sąsają bei užtikrinti operatyvų grįžtamąjį ryšį ir informacijos apie incidentus teikimą realiu laiku (angl. online), prieiga prie incidentų registravimo žurnalo ir incidentų registravimo teisės bus suteiktos nurodytiems Tiekėjo specialistams visam Paslaugų teikimo laikotarpiui.

4.5. Paslaugos turi būti teikiamos remiantis inkrementiniu-iteraciniu informacinių sistemų įgyvendinimo būdu (angl. Agile), kuomet sistemos savininko (angl. Product Owner) vaidmenį atlieka Pirkėjo paskiriamas asmuo, darbai planuojami vienos-dviejų savaičių iteracijomis, taikomos kitos atitinkamos praktikos darbų planavimui, prioretizavimui, komunikavimui, tarpinių ir galutinių rezultatų priėmimui.

4.6. Konkretūs susitarimai dėl taikomų inkrementinio-iteracinio įgyvendinimo būdo metodų ir praktikų (iteracijos trukmė, reguliarūs susitikimai, darbų sąrašų formatai, progreso vizualizavimas ir kt.) turi būti suderinti Paslaugų teikimo pradžioje.

4.7. Tiekėjas turi užtikrinti, kad siūlomos Paslaugos atitinka Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, nurodytus reikalavimus.

5. PASLAUGŲ UŽSAKYMO TVARKA

5.1. Techninėje specifikacijoje 1.5. papunktyje nurodytos Paslaugos teikiamos pagal Pirkėjo pateiktas konkrečias užduotis:

5.1.1. Pirkėjas užduotis Tiekėjui pateikia raštu (el. paštu arba registruojant užklausų valdymo sistemoje JIRA);

5.1.2. Tiekėjas Paslaugų įgyvendinimą pradeda tik gavęs Pirkėjo užsakymo patvirtinimą raštu (el. paštu arba užklausų valdymo sistemoje JIRA).

6. REIKALAVIMAI PASLAUGŲ TEIKIMO ETAPAMS

6.1. Paslaugų teikimo etapai ir teikimo terminai:

6.1.1. Techninės specifikacijos 1.5. papunktyje aprašytų paslaugų įgyvendinimas turės būti atliktas per 1 (vieną) mėnesį nuo konkretaus Užsakymo patvirtinimo dienos;

6.1.2. Vykdant kiekvieno etapo aprašyto Techninės specifikacijos 1.5. papunktyje atsparumo vertinimą ir įsilaužimo testavimą turi būti vykdomos tokios veiklos:

6.1.2.1. Atlikti visi etape suplanuoti testai nurodyti 3.1. papunktyje laikantis 3.2. papunktyje nurodytų reikalavimų;

6.1.2.2. Testavimas buvo atliktas naudojant tiek automatizuotus, tiek rankinius metodus;

6.1.2.3. Buvo užtikrinta testavimo sauga. Jei dėl testavimo veiksmų įvyko veiklos sutrikimai, įranga ar duomenys buvo atstatyti Tiekėjo sąskaita per ne ilgesnį nei 8 valandų laikotarpį nuo incidento nustatymo momento;

6.1.2.4. Buvo parengta ir pristatyta išsami testavimo ataskaita kaip nurodyta 3.3. papunktyje;

6.1.2.5. Atliktas pakartotinis testavimas. Patvirtinta, kad visos identifikuotos kritinės ir aukšto rizikos spragos buvo pašalintos. Atnaujinta testavimo ataskaita pateikta Pirkėjui.

6.1.3. Nustatoma, kad etapo atsparumo vertinimas ir įsilaužimo testavimas yra užbaigtas, kai:

6.1.3.1. atliktos visos 6.1.2 papunktyje numatytos veiklos ir Pirkėjas patvirtino užsakymo įvykdymą užsakymų žurnale (Jira arba kitoje Pirkėjo pasiūlytoje sistemoje);

6.1.3.2. atnaujinta (aktualizuota) testavimo ataskaita;

6.1.3.3. pakartotinio testavimo metu nenustatyta naujų trūkumų;

6.1.3.4. suderintas ir pasirašytas paslaugų perdavimo priėmimo aktas.

6.1.4. **Paslaugų teikimo terminai: visi AIVIKS įsilaužimų testavimo etapai turės būti įgyvendinti iki 2026 m. gruodžio 10 d., Paslaugų teikimo terminas gali būti pratęstas 6 mėn. laikotarpiui.**