



PAŽEIDŽIAMUMŲ SKANAVIMO ĮRANKIS SU DIEGIMU

TECHNINĖ SPECIFIKACIJA

1. SĄVOKOS IR SUTRUMPINIMAI

Pirkėjas – Atsakinga vandentvarkos asociacija „VANDENS JĖGA“, asociacijos narys.

(Pirkimą Pirkimo vykdytojo vardu atlieka AB „Klaipėdos vanduo“, juridinio asmens kodas 140089260, adresas Ryšininkų g. 11, Klaipėda, atstovaujanti atsakingą vandentvarkos asociaciją „Vandens jėga“).

Tiekėjas – ūkio subjektas – fizinis asmuo, privatusis juridinis asmuo, viešasis juridinis asmuo, kitos organizacijos ir jų padaliniai ar tokių asmenų grupė, su kuriuo Pirkėjas sudaro Sutartį.

Sutartis - sutartis, sudaroma tarp Tiekėjo ir Pirkėjo dėl Pirkimo objekto.

Techninė specifikacija arba TS – dokumentas, kuriame apibūdintas pirkimo objektas.

Prekės – TS nurodytas pirkimo objektas.

2. REIKALAVIMAI PIRKIMO OBJEKTUI

2.1. Esamos situacijos aprašymas.

Šiuo metu Asociacijos narių įmonės be specialių įrankių ir procesų neturi galimybių prevenciškai užkardyti, nustatyti ir reaguoti į kibernetinius incidentus. Siekiama įsigyti asociacijos nariams bendra automatinio valdymo dalies pažeidžiamumų skanavimo įrankį.

2.2. Bendrieji reikalavimai tiekėjui:

- 2.2.1. Tiekėjas prieš diegdamas sprendimą turės susiderinti diegimo grafikus su kiekvienu asociacijos narės paskirtu bendrovės atsakingu asmeniu.
- 2.2.2. Tiekėjas tiekdamas Prekes, teikdamas paslaugas ir atlikdamas darbus privalo vadovautis Lietuvos Respublikos kibernetinio saugumo įstatymu ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams valdantiems ypatingos svarbos informacinę infrastruktūrą, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2024 m. lapkričio 6 d. Nr. 945“ (galiojančiomis aktualiomis redakcijomis).
- 2.2.3. Pagal pateiktus reikalavimus diegėjas turi įsipareigoti be papildomo mokesčio realizuoti visus detalizuotinus techninius ir funkcinis reikalavimus (pvz., detalizuotas funkcijų vykdymo taisykles ir pan.). Taip pat diegėjo atsakomybė yra nemokamai pašalinti diegimo metu atsiradusius programinės įrangos ar jos įgyvendinimo trūkumus, jei diegėjas, teikdamas pasiūlymą ar atlikdamas projekto darbus, naudos analizės etape nesuderintas su perkančiąja organizacija sąvokas ar sutrumpinimus, kurie skirsis nuo perkančiosios organizacijos įsivaizdavimo ar supratimo, o tai sąlygos neteisingą ar nepilną reikalavimų supratimą bei realizavimą.
- 2.2.4. Įdiegto sprendimo galutinių naudotojo sąsaja savitarnos svetainėje turi būti pateikiama lietuviu kalba. Analitikų ir administratorių sąsajos sprendime pateikiamos anglų kalba.
- 2.2.5. Tiekėjas nemažiau kaip 36 mėnesių turi teikti gamintojo palaikymo paslaugas. Palaikymas pradedamas skaičiuoti nuo licencijų įsigijimo datos ir turi apimti incidentų valdymo funkcionalumo

Pirkimo objekto pavadinimas ¹	Pažeidžiamumų skanavimo įrankis
--	---------------------------------

3. PIRKIMO OBJEKTAS



Perkamas Kiekis^{II}		1 kompl.
Prekių pristatymo terminas (įskaitant diegimą ir kt. TS nurodytas paslaugas)		4 mėn.
Eil. Nr.	Savybė	Reikalaujami techniniai parametrai ar kita informacija
1.	Perkamas objektas	
1.1.	Gamintojas ir programinės įrangos pavadinimas	Nurodyti programinio sprendimo pavadinimą.
1.2.	Nuoroda į gamintojo techninę dokumentaciją	<ol style="list-style-type: none"> 1. Pateikti nuorodas į kiekvieno reikalavimo įgyvendinimo aprašymą gamintojo techninėje dokumentacijoje. 2. Jeigu siūlomas sprendimas susideda iš atskirų modulių, pateikti nuorodas į konkrečių sprendimo modulių techninę dokumentaciją.
1.3.	Programinės įrangos apibūdinimas	<p>Programinis sprendimas, turi leisti automatizuoti perkančiosios organizacijos pažeidžiamų valdymo procesą Technologiniuose tinkluose įskaitant:</p> <ul style="list-style-type: none"> • įrangos aptikimą, • pažeidžiamumų nustatymą, • klasifikavimą, • prioritetizavimą, • pažeidžiamumų šalinimo instrukcijų teikimą, • ataskaitų teikimą, <p>Automatinį informavimą apie nustatytus ir pašalintus pažeidžiamumus.</p>
1.4.	Licencijos	<p>Programinės įrangos licencija turi leisti:</p> <ol style="list-style-type: none"> 1.1. Surinkti informaciją apie visus vidinio operacinių technologijų tinklo (toliau – OT tinklo) įrenginius atliekant pasyvų skenavimą. 1.2. Surinkti informaciją apie visus aktyvius OT tinklo įrenginius, pasyviai analizuojant organizacijos vidinio OT tinklo srautą. 1.3. Centralizuotai valdyti pažeidžiamumus ne mažiau kaip 5 asociacijos įmonėse su ne mažiau kaip 22 objektuose; 1.4. Centralizuotai valdyti pažeidžiamumus ne mažiau kaip 3000 technologinio tinklo įrenginių; 1.5. Suteikti integracijos galimybes ir prieigą prie duomenų naudojant API.
1.5.	Sprendimo architektūra	<p>Siūlomas sprendimas turi:</p> <ol style="list-style-type: none"> 1.1. Būti realizuotas „On premises“ arba debesų kompiuterijos pagrindu; 1.2. Pagrindinė sprendimo valdymo konsolė turi būti prieinama per naršyklę; 1.3. Visi sprendimo komponentai, surinktus duomenys turi perduoti centralizuotai „On premises“ arba debesų kompiuterijos pagrindu veikiančiai sistemai, kurioje būtų vykdoma duomenų analizė ir valdymas; 1.4. Sistemos konfigūravimus, skenavimo rezultatų peržiūra, ataskaitų formavimus, ir kiti veiksmai turi būti atliekami centralizuotoje sistemoje; 1.5. Leisti atlikti vidinių įrenginių skenavimą naudojant vidinius virtualius skenavimo įrenginius;



		<p>1.6. Leisti pasyviai rinkti informaciją apie technologinio tinklo duomenų srautus.</p> <p>1.7. Gamintojas turi turėti virtualius skenerius ir pasyvius stebėjimo jutiklius skirtus šioms virtualizacijos platformoms: VMWare, Hyper-V;</p> <p>1.8. Gamintojas turi turėti fizinius pasyvaus stebėjimo jutiklių įrenginius.</p> <p>1.9. Gamintojas turi turėti virtualius skenerius.</p> <p>1.10. Automatiškai be vartotojo įsikišimo atsinaujinti visas duomenų bazes įskaitant visą informaciją apie pažeidžiamumus ir programinės įrangos gamintojų pateikiamus atnaujinimus;</p> <p>1.11. Turi būti galimybė sukurti įrenginių inventorių, apimančią tokius įrenginius kaip programuojami loginiai valdikliai (PLC), nuotoliniai terminalo įrenginiai (RTU), intelektualūs elektroniniai įrenginiai (IED), nuotoliniai IOs, žmogaus ir mašinos sąsajos (HMI), pramoniniai vartai, pastatų automatikos valdikliai, IP pagrindu veikiantys jutikliai, robotai, tvarkyklės (Drivers) ir kiti.</p>
1.6.	Prieigos kontrolė	<p>Turėti vartotojų rolėmis pagrįstą prieigą prie sistemos per interneto naršyklę.</p> <p>Rolių pagalba būtų galima valdyti vartotojo prieigą prie konkrečių duomenų rinkinių ir sistemos funkcijų.</p>
1.7.	Įrangos valdymas	<p>1.1. Sprendimas turi turėti funkcionalumą, leidžiantį struktūrizuoti informaciją apie organizacijos įrenginius, sukirstant juos pagal:</p> <p>1.1.1. Tinklus ir potinklius</p> <p>1.1.2. IP adresų režius</p> <p>1.1.3. Domenus</p> <p>1.1.4. Operacines sistemas</p> <p>1.2. Sprendimas turi leisti sukurti įrangos grupes, nurodyti įrangos funkciją, lokaciją, kritiškumą veiklai.</p> <p>1.3. Sprendimas turi turėti funkcionalumą leidžiantį įrangai suteikti žymes (angl. <i>tags</i>).</p> <p>1.4. Sprendimas turi leisti susikurti savo žymas.</p> <p>1.5. Sprendimas turi leisti įrangai priskirti neribotą kiekį žymų.</p> <p>1.6. Turi būti galimybė rankiniu būdu suteikti žymą įrangai.</p> <p>1.7. Turi būti galimybė automatinio/dinaminio būdu suteikinti įrangai žymas pagal pasirinktus atributus (pvz. identifikuota programinė įrangą, lokaciją, tipą, ir kt.) ir/arba jų kombinacijas.</p> <p>1.8. Sistema turi turėti funkcionalumą, leidžiantį aptikti nesankcionuotus įrenginius (angl. <i>rogue devices</i>)</p> <p>1.9. Turi būti galimybė sudaryti sankcionuotos ir nesankcionuotos programinės įrangos sąrašus.</p>
1.8.	Skenavimas	<p>1.10. Sprendimas turi turėti skirtingus skenavimo režimus:</p> <p>1.11. Skenavimas skirtas aptikti įrenginius;</p> <p>1.12. Skenavimas skirtas nustatyti pažeidžiamumus.</p> <p>1.13. Turi būti galimybė sukurti neribotą kiekį skenavimų, nurodant skenuojamą įrangą (pagal domenų, tinklus, potinklius, IP adresų režius, grupes ar grupių požymius).</p> <p>1.14. Turi būti galimybė sukurti skenavimų kalendorius, nurodant kiekvieno skenavimo dažnumą, pradžios laiką ir pabaigos laiką.</p>

		<p>1.15. Turi būti funkcionalumas, leidžiantis sukonfigūruoti individualius kiekvieno skanavimo nustatymus, įskaitant:</p> <p>1.16. Skenuojamus tinklus ir potinklius,</p> <p>1.17. Turi būti funkcionalumas, leidžiantis pašalinti istorinius skenavimo duomenis, jeigu įranga buvo neprieinama paskutinius x skenavimo kartus.</p> <p>1.18. Visi skenavimo duomenys turi būti saugomai centralizuotoje duomenų bazėje.</p> <p>1.19. Skirtingi skenavimai, skenuojantys tą pačią įrangą, turi papildyti centralizuotoje duomenų bazėje saugomus duomenis, o ne perrašyti juos.</p> <p>1.20. Skenavimo funkcionalumas turi naudoti OT tinklų vietinius (native) protokolus ir skenuoti tik nurodytus įrenginius (hostus), tikslingu (targeted) būdu.</p> <p>1.21. Sprendimas turi gebėti atlikti efektyvų pažeidžiamumų valdymą naudodamas tik pasyvų stebėjimą, su galimybe vykdyti aktyvų skenavimą, kai tai suteiktų papildomos naudos.</p> <p>1.22. Sprendimas neturi naudoti jokių trečių šalių skenerių pažeidžiamumams aptikti.</p>
1.9.	Technologinių įrenginių palaikymas	<p>1.1. Turi palaikyti šiuos OT tinklų įrenginių gamintojus: Rockwell Automation, Schneider Electric, Wago, Johnson Controls, ABB, , Eaton, Turck, Balluff, Distech Controls, Danfoss, Siemens ir kt.</p> <p>1.2. Turi palaikyti šiuos technologinių įrenginių protokolus:</p> <p>1.3. Siemens S7 Comm, Siemens S7 comm plus, Profinet, Ethernet IP, CIP (Common Industrial Protocol), PCCC, Modbus TCP, BACnet, Opto, DNP3, IEC 104, IEC 61850 – MMS, Beckhoff AMS / ADS, Omron Fins, Mitsubishi Melsoft, Mitsubishi CC Link, Mitsubishi SLMP, EtherCAT, Honeywell CeeNTComm (C200, C300), Emerson Delta-V, Microsoft Discovery Protocol, Schneider UMAS, Honeywell Centcomm, Proconos, GE-SRTP, MQTT, Phoenix Contact TCP 1962.</p> <p>1.4. Architektūros suderinamumas</p> <p>1.5. Sprendimas turi integruotis į esamą tinklo architektūrą, pagrįstą Purdue modeliu (nuo 0 iki 5 lygio).</p> <p>1.6. Turi būti palaikomi tiek pasyvieji, tiek aktyvieji įrenginių atradimo metodai, pritaikyti skirtingiems tinklo segmentams pagal jautrumą.</p> <p>1.7. Sprendimas turi sudaryti išsamią įrenginių inventORIZaciją, naudodamas:</p> <p>1.8. Pasyvius tinklo jutiklius Purdue 0–2 lygio įrenginiams (pvz., PLC, HMI, RTU, SCADA).</p> <p>1.9. Saugius aktyvius skenavimus 2–3.5 Purdue lygio segmentuose</p> <p>1.10. Aptikimo funkcionalumas turi identifikuoti įrenginio tipą, gamintoją, programinės įrangos versiją ir operacinę sistemą, nepažeidžiant įrenginio veikimo.</p> <p>1.11. Pažeidžiamumo valdymas</p> <p>1.12. Sprendimas turi palaikyti pasyvų pažeidžiamumų nustatymą jautriuose Purdue lygiuose (0–2).</p> <p>1.13. Turi būti užtikrintas saugus aktyvų pažeidžiamumų skenavimas mažiau jautriuose lygiuose Purdue (3–3.5), nedarant įtakos įrenginiams.</p>



1.10.	Pasyvūs jutikliai (sensors)	<p>1.1. Sprendimas turi palaikyti veidrodinį tinklo srautą, naudodamas SPAN, RSPAN ir ERSPAN metodus arba fizinius TAP įrenginius.</p> <p>1.2. Sprendimas turi turėti pasyviuosius jutiklius, kurie leistų:</p> <ul style="list-style-type: none"> 1.2.1. stebėti tinklą be aktyviųjų veiksmų 1.2.2. automatiškai aptikti ir atpažinti visus tinklo įrenginius, tiek žinomus, tiek nežinomus, 1.2.3. nustatyti pagrindinius įrenginių atributus, priskirti juos OS ar aparatūros kategorijoms, identifikuoti tinklo srautą ir ryšį tarp įrenginių. 1.2.4. Skenavimo funkcionalumas turi naudoti OT tinklų vietinius (native) protokolus ir skenuoti tik nurodytus įrenginius (hostus), tikslingu (targeted) būdu. 1.2.5. Sprendimas turi gebėti atlikti efektyvų pažeidžiamumų valdymą naudodamas tik pasyvų stebėjimą, su galimybe vykdyti aktyvų skenavimą, kai tai suteiktų papildomos naudos 1.2.6. Sprendimas turi užtikrinti efektyvų pažeidžiamumų valdymą su rizika grįstu (risk based) prioritetų nustatymu ir grėsmių aptikimą, paremtą grėsmių žvalgyba (Threat intelligence detection).
1.11.	Duomenų dedubliavimas	<p>Sprendimas turi turėti dedubliavimo procesą, skirtą pakartotinai aptiktiems įrenginiams, įvertintiems pagal šiuos kriterijus:</p> <ul style="list-style-type: none"> siūlomo sprendimo sugeneruotą unikalų ID, MAC adresą, įrenginio pavadinimą, IP adresą. <p>Sprendime turi būti galimybė nurodyti įrenginio pavadinimus, kurių pasyvūs jutikliai neįtrauktų į dedubliavimo procesą.</p>
1.12.	Technologinių įrenginių konfigūracijos tikrinimas	<p>Turi būti galimybė importuoti šių gamintojų technologinių įrenginių konfigūracijų failus:</p> <p>Emerson, Emerson/GE Fanuc Automation, Rockwell, Siemens, Schneider, Mitsubishi</p> <p>Turi būti galimybė importuoti šiuos technologinių įrenginių konfigūracijų failų formatus:</p> <p>zip, .tnzip, .tsm, .wsm, .fhx, .SwxCF, .cpx, .RSS, .l5x, .rsh, .xml, .cfg, .zap, .lnp, .mnp, .zef, .xef, .xtwd, .ccf, .smbp, .prx, .gx3, .gxw, .cd3, .cd31, .cd32.</p>
1.13.	Pažeidžiamų vertinimas	<p>1.1. Sprendimas turi aptikti ir reitinguoti problemas, riziką ir pažeidžiamumą. Jis taip pat turi pateikti išsamią informaciją apie rizikos pobūdį ir rekomendacijas jai sumažinti;</p> <p>1.2. Sprendimas turi būti suderinamas su CVE (angl. <i>Common Vulnerabilities and Exposures</i>) (https://cve.mitre.org/) ir turėti teikti ne mažiau kaip 10 metų CVE pažeidžiamumų archyvą;</p> <p>1.3. CVSS kontekste, sprendimas turi pateikti kiekvieno pažeidžiamumo prioritetą, atsižvelgiant į OT rizikos svarbumą.</p> <p>1.3. Sprendimas turi naudoti pažeidžiamumo išnaudojimo informaciją iš trečiųjų šalių, įskaitant, bet ne apsiribojant šiais šaltiniais:</p>

		<p>1.3.1. Kibernetinės saugos ir infrastruktūros saugos agentūros (angl. CISA - The Cybersecurity and Infrastructure Security Agency) žinomų išnaudotų pažeidžiamumų katalogas (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)</p> <p>1.3.2. MITRE ATT&CK Framework (https://attack.mitre.org/)</p> <p>1.4. Sprendimas turi pateikti informaciją apie žinomus parengtus pažeidžiamumų išnaudojimus (angl. exploits).</p> <p>1.5. Sprendimas turi pateikti informaciją apie žinomą kenkėjišką programinę įrangą išnaudojančią pažeidžiamumą (angl. malware).</p> <p>1.6 Sprendimas turi sekti pažeidžiamumo aptikimo ir stebėjimo datas, kurias galima naudoti filtruojant ir rengiant ataskaitas tam tikram laiko tarpui.</p> <p>1.7 Sprendimo gamintojas turi būti sertifikuota CVE numeracijos institucija (angl. CVE Numbering Authority) ir prisidėti prie MITRE Common Vulnerabilities and Exposures sąrašo.</p>
1.14.	Pažeidžiamų šalinimas	<p>1.1. Turi būti galimybė pažymėti aptiktą pažeidžiamumą, kaip pažeidžiamumą su kurio egzistavimu ir jo keliamą riziką perkančioji organizacija susitaiko – „priima riziką“ ir neplanuoja imtis šalinimo veiksmų.</p> <p>1.2. Turi būti galimybė palikti komentarus prie „priimtos rizikos“ pažeidžiamumų.</p> <p>1.3. Sprendimas turi turėti incidentų registravimo ir valdymo funkcionalumą.</p> <p>1.4. Turi būti funkcionalumas, leidžiantis aptikus pažeidžiamumą sukurti sistemoje incidentą, kuris būtų automatiškai priskiriamas įrangos savininkui/valdytojui ar kitam sprendimo naudotojui.</p> <p>1.5. Turi būti funkcionalumas, kuris automatiškai uždarytų incidentą kai nustatoma, kad pažeidžiamumas buvo pašalintas.</p> <p>1.6. Sprendimas turi automatiškai diegti programinės įrangos atnaujinimus, kurie pašalintų aptiktus pažeidžiamumus.</p> <p>1.7. Sprendimas turi pateikti praktinius pažeidžiamumų sušvelninimo patarimus, padedančius operatoriams sumažinti pažeidžiamumo keliamą riziką jo neužlopanč (without patching).</p>
1.15.	Ataskaitos	<p>1.1. Sprendimas turi turėti funkcionalumą rengti skirtingo detalumo ataskaitas skirtingoms naudotojų grupėms: administratoriams, saugumo ekspertams, vadovams ir kt.</p> <p>1.2. Turi turėti funkcionalumą, leidžiantį parengti ataskaitų šablonus.</p> <p>1.3. Turi būti funkcionalumas, leidžiantis filtruoti duomenis pagal skirtingus atributus ar jų kombinacijas.</p> <p>1.4. Ataskaitų formatai - PDF, XML, HTML.</p>
1.16.	Skaitlentės (angl. Dashboards)	Sprendimas turi turėti skaitlentes skirtas atvaizduoti informaciją realiu laiku.



		<p>Naudotojai turi turėti funkcionalumą, leidžiantį susikurti personalizuotas skaitlentes.</p> <p>Naudotojai turi turėti galimybę dalintis savo sukurtoms skaitlentėmis su kitais sprendimo naudotojais.</p> <p>Sprendimas turi užtikrinti techninį resursą, kuris padėtų perkančiajai organizacijai pritaikyti ar sukurti naujus informacinius skydelius (angl. dashboards)</p>
1.17.	Duomenys	<p>Sprendimas turi užšifruoti duomenis, kurie nėra naudojami (angl. at rest).</p> <p>Sprendimas turi užšifruoti visus perduodamus duomenis;</p> <p>Sprendimo duomenys turi būti saugomi Europos sąjungos valstybėse esančiame duomenų centre.</p>
1.18.	Programinės įrangos atnaujinimų valdymas	Sprendimas turi automatiškai koreliuoti aptiktus pažeidžiamumus su reikiamais atnaujinimais.
1.19.	Nuolatinis tinklo stebėjimas	<p>1.5. Turi užtikrinti, kad organizacija būtų savalaikiai informuojama apie:</p> <ul style="list-style-type: none"> 1.5.1. Tinkle aptikus naujus įrenginius, 1.5.2. Aptiktus ypatingos svarbos pažeidžiamumus, 1.4.3. Grėsmių aptikimas, naudojant žvalgybine informacija (angl. Intelligence) pagrįstus aptikimo metodus 1.4.4 Sprendimas turi atnaujinti grėsmių aptikimo ir pažeidžiamumų parašus ne rečiau kaip kartą per savaitę
1.20.	API	<p>1.1. Sprendimas turi turėti integracijoms skirtą API, kurio pagalba būtų galima:</p> <ul style="list-style-type: none"> 1.1.1. Valdyti įrenginių, įrenginių grupių, tinklų/potinklų, IP adresų, sąrašus, 1.1.2. Papildyti ar atnaujinti įrenginių, įrenginių grupių, tinklų/potinklų, IP adresų, sąrašus, 1.1.3. Valdyti skenavimo darbus, 1.1.4. Gauti informaciją apie aptiktus pažeidžiamumus, 1.1.5. Valdyti naudotojus ir jų teisę, keisti naudotojų slaptažodžius, 1.1.6. Gauti informacija apie vartotojų atliktus veiksmus, 1.1.7. Valdyti tinklo stebėjimo taisykles
1.21.	Mokymai	<p>Tiekėjas turi suteikti gamintojo mokymus ne mažiau kaip trims darbuotojams.</p> <p>Jeigu gamintojas turi Online mokymų platformą tiekėjas turi užtikrinti, kad ne mažiau kaip trims darbuotojams turėtų prieigą prie šios platformos.</p>
1.22.	Dokumentacija	<p><u>Su prekėmis turi būti pateikta:</u></p> <ul style="list-style-type: none"> 1 Prekių važtaraštis su nurodytu Prekių pavadinimu ir kiekiu; 2. Prekių perdavimo - priėmimo aktas; 3. Įrangos techninį pasą lietuvių arba anglų kalba; 4. Gamintojo ar jo oficialaus atstovo išduotos Prekių atitikties deklaracijos (sertifikatai) lietuvių arba anglų kalba. 5. Prekių montavimo ir naudojimo instrukcijos lietuvių arba anglų kalba; 6. Prieš montuojant Prekes, pateikti įrangos struktūrinės ir principinės schemas suderinimui.
1.23.	Trūkumų šalinimas	<p>Prekių perdavimo - priėmimo ar Garantinio laikotarpio metu pastebėtiems trūkumams šalinti nustatomas 10 (dešimt) darbo dienų terminas nuo Pirkėjo pranešimo apie sugedusias,</p>



		<i>nekokybiškas ar turinčias trūkumų Prekes. Tiekėjas netinkamas/sugedusias Prekes privalo pasiimti iš Pirkėjo nurodytų adresų ir suremontuotas Prekes savo lėšomis grąžinti Pirkėjo nurodytais adresais, iš kurių jos buvo paimtos.</i>
1.24.	Prekių pristatymo vieta	<p>UAB „Vilniaus Vandenys“: Spaudos g. 8-1, Vilnius, 05132.</p> <p>UAB „Kauno vandenys“: Aukštaičių g. 43, Kaunas, 44158 Kauno m. sav.</p> <p>UAB „Dzūkijos vandenys“: Pulko g. 75, Alytus, 62135 Alytaus m. sav.</p> <p>UAB „Utenos vandenys“: Vandenų gatvė 1, Naujasodžio kaimas, 28113 Utena; Palijoniškio gatvė 22, 28180 Utena; AB „Klaipėdos vanduo“: Ryšininkų 11, Klaipėda.</p>
1.25.	Kokybė	<i>Tiekėjas, teikdamas pasiūlymą patvirtina, kad parduodamos Prekės yra tinkamos naudoti pagal jų tikslinę paskirtį, kad nėra paslėptų Prekių trūkumų, dėl kurių Prekių nebūtų galima naudoti pagal jų tikslinę paskirtį arba dėl kurių sumažėtų Prekių naudingumas.</i>
2.	Tiekėjo kartu su prekėmis atliekamos (-i) paslaugos/darbai:	
2.1.	Tiekėjas turės	<ol style="list-style-type: none"> 1. Tiekėjas turės pateikti diegimo grafiką ir suderinti su Pirkėjo atstovais. 2. Tiekėjas turi pateikti techninę dokumentaciją apie sistemos diegimą, administravimą ir naudojimą anglų kalba ar lietuvių kalba. Tiekėjas turi diegti ir sukonfigūruoti programinę įrangą serveriuose bei pateikti klientui techninę ir eksploatacinę platformos dokumentaciją. Tiekėjas privalo suteikti ne mažiau kaip 20 valandas konsultacijų, (workshop principu) kurių metu tiekėjas turės suteikti konsultacijas šiais klausimais: Virtualių skenerių diegimas, Skenavimo konfigūracijų rengimas, Įrenginių struktūrizavimas, Ataskaitų šablonų parengimas, Skaitlenčių konfigūravimas, Pranešimų konfigūravimas, Atnaujinimo periodinių darbų konfigūravimas. 3. Kitoms su siūlomų sprendimų susijusiomis paslaugomis. 4. Tiekėjas turi suteikti konsultavimo ir mokymo paslaugas kliento techniniams specialistams (ne mažiau 15 asmenims) dėl Sistemos administravimo ir eksploataavimo (ne mažiau kaip 40 valandų) anglų, lietuvių – klausimais: Virtualių skenerių diegimas, Skenavimo konfigūracijų rengimas, Įrenginių struktūrizavimas, Agentų diegimas, Ataskaitų šablonų parengimas, Skaitlenčių (dashboard) konfigūravimas, Pranešimų konfigūravimas, Atnaujinimo periodinių darbų konfigūravimas, kitoms su siūlomų sprendimų susijusiomis paslaugomis. 5. Tiekėjas turės pasirūpinti SSL sertifikatais 36 mėn. laikotarpiu, jei sistemos atskirai to reikalauja. 6. Tiekėjas turi pateikti ir sudiegti visą reikalingą programinę įrangą (OS, virtualizavimo platforma ir kitą programinę įrangą reikalingą sprendimui) reikalinga, kad sistema (sprendimas) tinkamai veiktų. Pirkėjas neapteikia jokių licencijų, visas reikalingas licencijas sprendimo veikimui pateikia Tiekėjas.



		7. Tiekėjas turi teikia sistemos palaikymo ir talpinimo paslaugas (jei tokios reikalingos) ne mažiau kaip 36 mėn.
2.2.	Garantija suteiktoms Paslaugoms/Darbams	Ne trumpesnė kaip 36 mėn. nuo priėmimo-perdavimo dokumento pasirašymo
3.	Žalieji reikalavimai prekėms	
3.1.	Nustatomi žalieji reikalavimai prekėms	Perkamas nematerialaus pobūdžio prekė
4.	Kiti reikalavimai	
1.1.	Tiekėjas turi užtikrinti, kad Įrangos gamintojas nėra paskelbęs apie siūlomos Įrangos gamybos arba tobulinimo nutraukimą (pvz. „End of life time“ ar „Discontinued“).	
1.2.	Visa pateikiama įranga privalo būti ne prastesnių parametrų nei nurodyta šioje specifikacijoje arba geresnių parametrų.	

ⁱ Jeigu techninėje specifikacijoje yra nurodytas konkretus perkamos prekės tipas, modelis, ženklas, taikomas standartas ar kita konkreti apibūdinanti informacija, Pirkėjui yra priimtina lygiavertė prekė, atitinkanti techninėje specifikacijoje nurodytos prekės parametrus ar taikomus standartus.

Šiame dokumente vartojami terminai „turi būti“, „turi turėti“, „turi leisti“, „turi būti galimybė“, „turi būti sukurtas (-a)“ yra lygiaverčiai ir reiškia, kad Tiekėjas pirkimo apimtyje privalo sukurti ir įdiegti (ar pateikti ir įdiegti) atitinkamą funkcionalumą ar suteikti atitinkamas paslaugas. Funkcionalumas, kuris yra nurodytas būsimoju laiku (bus, leis, apims ir t.t.) nurodo siekiamą įgyvendinti būseną ir reiškia, kad Tiekėjas pirkimo apimtyje privalo sukurti ir įdiegti (ar pateikti ir įdiegti) atitinkamą funkcionalumą.

ⁱⁱ Kai nurodytas tikslus Prekių kiekis, Pirkėjas įsipareigoja išpirkti visą nurodytą prekių kiekį.