

ADMS SCADA
software
maintenance services
technical specification

ADMS SCADA
programinės įrangos
prižiūros paslaugų
techninė specifikacija

TABLE OF CONTENTS/ TURINYS

1. CONCEPTS	32
1. Sąvokos.....	3
2. PROCUREMENT OBJECT.....	4
2. Pirkimo objektas.....	4
3. EXISTING SYSTEM CHARACTERISTICS.....	4
3. Esama sistemos charakteristika	4
4. REQUIREMENTS FOR THE PROCUREMENT OBJECT.....	5
4. Reikalavimai pirkimo objektui	5
5. DOCUMENTS TO BE SUBMITTED WITH THE TENDER.....	Error! Bookmark not defined.
5. Sutarties vykdymo metu teikiami dokumentai	12
6. SERVICE PROCEDURE	13
6. Paslaugų teikimo tvarka	13
7. MATRIX OF RESPONSIBILITIES.....	15
7. Atsakomybių matrica.....	15
8. ATTACHMENTS.....	
8. Priedai.....	

DESCRIPTION OF THE PROCUREMENT OBJECT		PIRKIMO OBJEKTO APRAŠYMAS
1. CONCEPTS		1. SĄVOKOS
1.1.	Buyer shall mean AB "LTG Infra".	Pirkėjas – AB „LTG Infra“.
1.2.	Supplier shall mean an economic entity – natural person, private legal entity, public legal entity, other organisations and their divisions or a group of such persons with whom the Buyer enters into a Contract.	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.
1.3.	Contract shall mean a Contract concluded between the Supplier and the Buyer concerning the object of the Procurement.	Sutartis – Sutartis, sudaroma tarp Tiekėjo ir Pirkėjo dėl Pirkimo objekto.
1.4.	System shall mean GE Grid ADMS SCADA	Sistema – GE Grid ADMS SCADA
1.5.	Maintenance shall mean the system support (troubleshooting), preventive work and consulting services.	Priežiūros paslaugos – Sistemos palaikymo (sutrikimų nustatymas ir jų pašalinimas), profilaktiniai darbai ir konsultavimo paslaugos.
1.6.	System malfunctions - Software malfunctions that are felt by the user, make it difficult to work with the system, work with the system becomes impossible, the function does not perform, does not properly perform its purpose, incorrect or unrealistic data is distorted, the format of the data provided does not comply with the agreed solutions, any information is lost.	Sistemos sutrikimai - Programinės įrangos veikimo sutrikimai, kurie juntami naudotojui, apsunkina darbą su sistema, darbas su sistema tampa neįmanomas, funkcija neatlieka, netinkamai atlieka savo paskirtį, iškraipomi, pateikiami neteisingi, tikrovės neatitinkantys duomenys, pateikiamų duomenų formatas neatitinka suderintiems sprendimams, prarandama bet kokia informacija.
1.7.	Normal System Operation - the system is operating at full capacity in the manufacturer's intended configuration, all system parts and processes are functioning to their full extent, and there are no deviations from the intended system operating parameters.	Normalus Sistemos veikimas - sistema veikia pilnu pajėgumu gamintojo numatytoje konfigūracijoje, visos sistemos dalys ir procesai funkcionuoja pilnoje apimtyje bei nėra nukrypimų nuo numatytų sistemos veikimo parametrų.
1.8.	Response time – the period of time from the receipt of any agreed notification from the Buyer until the initiation of its decision.	Reakcijos laikas – laiko tarpas nuo bet kokio sutarto pranešimo iš Pirkėjo gavimo iki jo sprendimo pradžios.
1.9.	Resolution time/ Troubleshooting time - the time period from receipt of any agreed a notification from the Customer to the troubleshooting and restoration of full functionality.	Sprendimo laikas/ Sutrikimo šalinimo laikas - laiko tarpas nuo pranešimo iš Pirkėjo gavimo iki sutrikimo pašalinimo, pilno funkcionalumo atstatymo.
1.10.	System software shall mean the application, DB, services, dynamic link libraries, protocol libraries, etc.	Sistemos programinė įranga – aplikacija, DB, servisai, dinaminiai nuorodų bibliotekos, protokolų bibliotekos ir t.t.
1.11.	L1 - System support level for event registration and transmission.	L1 - Sistemos palaikymo lygis, skirtas įvykių registracijai ir perdavimui.
1.12.	L2 - System support level responsible for the system's IT infrastructure and user workstations.	L2 - Sistemos palaikymo lygis, atsakingas už sistemos IT infrastruktūrą ir naudotojų darbo vietas.
1.13.	L3 - System support level that determines the cause of the malfunction and is responsible for communication with the supplier.	L3 - Sistemos palaikymo lygis, nustatantis sutrikimo atsiradimo priežastį ir atsakingas už komunikaciją su tiekėju.

1.14.	L4 - System support level responsible for the periodic assessment of system vulnerabilities and their elimination, timely restoration of operation, identification of the causes of the malfunction and its elimination.	L4 - Sistemos palaikymo lygis, atsakingas už sistemos periodinį pažeidžiamumų vertinimą ir jų šalinimą, savalaikį veikimo atstatymą, sutrikimo priežasčių nustatymą ir jo pašalinimą.
1.15.	Critical Error shall mean a technical, logical and similar error that prevents further use of the system.	Kritinė klaida – techninė, loginė ir pan. klaida, kuri stabdo tolimesnį Sistemos naudojimą.
1.16.	Error shall mean a situation when an error message is received in the system or the functionality of the system does not meet the set requirements.	Klaida – situacija, kai sistemoje gaunamas klaidos pranešimas arba sistemos funkcionalumas neatitinka nustatytų reikalavimų.
1.17.	Warning level malfunctions are failure that does not affect the normal provision of services, does not confuse the system user, does not affect the operation of software, hardware and peripheral equipment or its operational characteristics.	Ispėjimo lygio sutrikimas - sutrikimas, kuris neturi įtakos normaliam paslaugų teikimui, neklaidina sistemos naudotojo, neturi įtakos programinės, techninės ir periferinės įrangos veikimui ar jos eksploatacinėms savybėms.
1.18.	RTU shall mean the remote terminal units.	TSPĮ – teleinformacijos surinkimo perdavimo įrenginiai.
1.19.	EVKS shall mean the LTG traffic control system.	EVKS – LTG eismo valdymo sistema.
2. PROCUREMENT OBJECT		2. PIRKIMO OBJEKTAS
2.1.	Procurement object – ADMS SCADA software maintenance services.	2.1. Pirkimo objektas – ADMS SCADA programinės įrangos priežiūros paslaugos.
2.2	System maintenance shall consist of: troubleshooting; preventive works; system update; consultations, the right to contact the manufacturer in case of an issue	2.2. Sistemos priežiūrą sudaro: 2.2.1. Sutrikimų šalinimas; 2.2.2. Profilaktiniai darbai; 2.2.3. Atnaujinimų diegimas; 2.2.4. Konsultacijos, teisė kreiptis į gamintoją iškilus problemai.
2.3.	The responsibilities between the buyer and the supplier regarding the object of purchase are presented in Section No. 8 of this document, "Matrix of Responsibility".	Atsakomybės tarp pirkėjo ir tiekėjo dėl pirkimo objekto pateiktos šio dokumento skyriuje Nr. 7 „Atsakomybių matrica“.
3. EXISTING SYSTEM CHARACTERISTICS		3. ESAMA SISTEMOS CHARAKTERISTIKA
3.1.	Number of system point\signal licences – 40000 pcs.	Sistemos taškų\signalų licencijų skaičius – 40000 vnt.
3.2.	The number of user licenses is 10, of which 5 are with management rights and 5 are without management rights. The licenses are permanent.	Naudotojų licencijų skaičius – 10 vnt., iš jų 5 vnt. yra su valdymo teise ir 5 vnt. be valdymo teisės. Licencijos yra nuolatinės.
3.3.	Application version: v6.9.2.0.10	Aplikacijos versija: v6.9.2.0.10
3.4.	The system runs on the following operating systems with regular security updates: - Microsoft Windows 2022; - Microsoft Windows 11 Enterprise; - Linux RedHat Enterprise Linux 8;	Sistema veikia šiose operacinėse sistemose su reguliariais saugumo naujinimais: - Microsoft Windows 2022; - Microsoft Windows 11 Enterprise; - Linux RedHat Enterprise Linux 8;
3.5.	Database: Oracle sqlplus, version 19.27.0.0.0	Duomenų bazė: Oracle sqlplus, versija 19.27.0.0.0

3.6.	The supplier must provide all licenses required for the DB to ensure functionality.	Tiekėjas turi pateikti visas DB reikalingas licencijas funkcionalumui užtikrinti.
3.7.	The System user accounts shall be managed via Customer's managed Active Directory (AD) system or Entra ID, enabling Single Sign On (SSO) principles and supporting at least one of the following authentication protocols: Open ID Connect, SAML 2.0, WS-Fed. System default/built-in accounts shall be disabled and available for use only in exceptional cases (such as system upgrade or disaster recovery).	Sistemos naudotojų paskyros turi būti valdomos per Pirkėjo valdomą aktyvaus katalogo (angl. Active Directory (AD)) arba Entra ID sistemas, užtikrinant vieno prisijungimo (angl. Single Sign On (SSO)) principus ir autentikavimui naudojant bent vieną iš šių protokolų: Open ID Connect, SAML 2.0, WS-Fed. Sistemos vidinės (default, built-in) naudotojų paskyros turi būti užblokuotos ir galės būti naudojamos tik išskirtiniais atvejais (pvz. sistemos atnaujinimas ar atstatymas).
3.8.	System transmit the catenary status to the EVKS: there is voltage, there is no voltage, not controlled. System must receive the following data from EVKS: a) the position of the train on the electrified track; b) train number.	Sistema perduoda į EVKS kontaktinio tinklo būseną: yra įtampa, nėra įtampos, nekontroliuojama Sistema priima iš EVKS šiuos duomenis: a) traukinio padėtis elektrifikuotame kelyje; b) traukinio numeris.
3.9.	IEC 60870-5-104 data exchange protocol license is used between the system and RTU.	Naudojama IEC 60870-5-104 duomenų apsikeitimo protokolo licencija tarp sistemos ir TSPĮ.
3.10.	The system has a test (Pre-PROD) environment	Sistema turi testinę (Pre PROD) aplinką
4. REQUIREMENTS FOR THE PROCUREMENT OBJECT		4. REIKALAVIMAI PIRKIMO OBJEKTUI
4.0.1.	The services must not pose a threat to national security, as specified in the procurement documents.	Paslaugos turi nekelti grėsmės nacionaliniam saugumui, kaip tai nurodyta Pirkimo dokumentuose.
4.0.2.	The supplier must ensure the proper functioning of the system, which is described in Section No. 4 of this document, "Requirements for the procurement object".	Tiekėjas turi užtikrinti tinkamą sistemos veikimą, kuris yra aprašytas šio dokumento skyriuje Nr. 4 „Reikalavimai pirkimo objektui“.
4.1. System troubleshooting		4.1. Sistemos sutrikimų šalinimas

4.1.1.	Response times and troubleshooting deadlines				Reakcijos laikai ir sutrikimų šalinimo terminai			
	Malfunction classification	Response time	Malfunction elimination deadline	Service supply time	Sutrikimo klasifikacija	Reakcijos laikas	Sutrikimo pašalinimo terminas	Paslaugų tiekimo laikas
	Critical error	15 min	3 hours	365×7×24	Kritinė klaida	15 min	3 valandos	365×7×24
	Error	30 min	8 hours	365×7×24	Klaida	30 min	8 valandos	365×7×24
	Warning	30 min	7 days	365×5×8	Ispėjimas	30 min	7 dienos	365×5×8
	Consulting	30 min	7 days	365×5×8	Konsultacija	30 min	7 dienos	365×5×8
4.1.2.	System must operate continuously 24 (twenty-four) hours a day, 7 (seven) days a week.				Sistema turi nepertraukiamai veikti 24 (dvidešimt keturias) valandas per parą 7 (septynias) dienas per savaitę.			
4.1.3.	End-users must be guaranteed system availability reaching 99.5% of the total calendar time per year. System downtime due to IT infrastructure failures shall not add up.				Galutiniams naudotojams turi būti užtikrinamas sistemos prieinamumas siekiantis 99,5% viso kalendorinio laiko per metus. Sistemos sutrikimų laikas dėl IT infrastruktūros gedimų nesumuojamas.			
4.1.4.	In the event of malfunctions in the system's interfaces with integrated systems, the Supplier must: 1. resolve the issues if they are related to changes or solutions implemented by the Supplier; or 2. provide a detailed technical analysis demonstrating that the issues do not fall under Supplier's responsibility. The analysis must be submitted in writing, specifying the causes, evidence, and recommendations for further actions.				Atsiradus sistemos sąsajų su integruotomis sistemomis veikimo sutrikimams, Tiekėjas privalo: 1. pašalinti gedimus, jei jie susiję su Tiekėjo įgyvendintais pakeitimais ar sprendimais; arba 2. pateikti išsamią techninę analizę, pagrindžiančią, kad gedimai nėra susiję su Tiekėjo atsakomybe. Analizė turi būti pateikta raštu, nurodant priežastis, įrodymus ir rekomendacijas dėl tolimesnių veiksmų.			
4.1.5.	Supplier shall be responsible for managing the database.				Tiekėjas atsakingas už duomenų bazės valdymą			
4.2. Preventive works					4.2. Profilaktiniai darbai			
4.2.1.	System must create and save backup copies of all stored data during runtime and non-runtime periods and at the same time meeting the performance requirements and not interfering work with the system.				Sistema turi kurti ir saugoti visų saugomų duomenų atsargines kopijas tiek veikimo, tiek neveikimo laikotarpiais ir tuo pačiu atitikti našumo reikalavimus bei netrukdyti dirbti su sistema.			
4.2.2.	When creating a backup or archive of the system, an integrated copy of the data must be stored, Transactions still pending in system and incomplete processed data must not be included, and the ongoing processes and transactions must not be terminated				Rengiant sistemos rezervinę kopiją arba archyvą, į archyvą turi patekti integrali duomenų kopija, t.y. neturi būti įtrauktos sistemos dar vykdomos transakcijos ir nebaigti apdoroti duomenys, o vykdomi procesai ir transakcijos neturi būti nutrauktos.			

4.2.3.	The high-availability solution must operate automatically in the event of incidents — ensuring service continuity without human intervention. Human involvement may only be required to restore the system to its previous state if automatic recovery does not cover all configuration or data aspects.	Aukšto prieinamumo sprendimas turi veikti automatiškai incidentų atveju - t. y. užtikrinti paslaugų tęstinumą be žmogaus įsikišimo. Žmogaus įsitraukimas gali būti reikalingas tik tam, kad būtų atstatyta sistemos būklė į tokia, kokia buvo prieš incidentą, jei automatinis atkūrimas neapima visų konfigūracinių ar duomenų aspektų.
4.2.4.	High availability Solution must ensure RPO (English Recovery point objective) – 15 minutes, RTO (English Recovery time objective) – 1 hour. (when the same or better level of service provision is ensured by the infrastructure of the data center).	Aukšto prieinamumo Sprendimas turi užtikrinti RPO (angl. Recovery point objective) – 15 min., RTO (angl. Recovery time objective) – 1 val. (kai tokį ar geresnį paslaugų teikimo lygį užtikrina duomenų centro infrastruktūra).
4.2.5.	The system must retain application logs in the production environment for a minimum of 3 years and infrastructure and service metrics for a minimum of 6 months to enable incident investigation and compliance needs.	Sistema privalo saugoti programų žurnalus gamybinėje aplinkoje ne trumpiau kaip 3 metus, o infrastruktūros ir paslaugų metriką – ne trumpiau kaip 6 mėnesius, kad galėtų atlikti incidentų tyrimą ir atitikties poreikius.
4.2.7.	System must be able to monitor the storage period of a record and select records for deletion automatically.	Sistema turi turėti galimybę stebėti įrašo saugojimo terminus ir automatiškai atrinkti įrašus naikinimui suėjus terminui.
4.2.8.	The system must be able to automatically initiate the deletion of records after their retention period has expired.	Sistema turi turėti galimybę automatiškai inicijuoti įrašų ištrynimą pasibaigus jų saugojimo terminui.
4.2.9.	Once a year, the supplier must provide documents proving that the system does not have critical, high and medium-level cyber vulnerabilities detected by a scan performed by the NKSC or when the scan is performed by one of the TOP 10 professional vulnerability scanning tools prevailing on the market, evaluated by independent parties, including Gartner, Forrester or others.	Vieną kartą metuose tiekėjas turi pateikti įrodančius dokumentus, kad sistema neturi kritinių, aukšto ir vidutinio lygio kibernetinių pažeidžiamumų, aptiktų NKSC atliktų skenavimu arba kai skenavimas yra atliktas vienu iš TOP 10 vyraujančių rinkoje profesionalių pažeidžiamumų skenavimo įrankių, įvertintu nepriklausomų šalių, t.k. Gartner, Forrester ar kt.
4.2.10.	The system must support event-based alarm generation and reporting when critical operational changes or incidents are detected, or support passive state check probes that periodically monitor the status of the system components and report any disruptions.	Sistema turi palaikyti įvykiais paremtą aliarmų generavimą ir ataskaitų teikimą, kai nustatomi kritiniai veikimo pokyčiai ar incidentai, arba palaikyti pasyviuos būklės patikrinimo zondus, kurie periodiškai tikrina sistemos komponentų būklę ir praneša apie sutrikimus.
4.2.11.	The Buyer shall monitor the system via the Zabbix platform. If necessary, the Buyer shall provide the Supplier with access to view messages in the Zabbix console and configure incident notification by e-mail.	Sistemos stebėseną pirkėjas vykdo per Zabbix platformą. Esant poreikiui Pirkėjas suteiks Tiekėjui žinučių peržiūros prieigą Zabbix konsolėje ir sukonfigūruos incidentų informavimą el. paštu.
4.2.12.	The system monitoring rules and recommendations are developed by the supplier. The buyer integrates the rules into the Zabbix platform.	Sistemos stebėsenos taisyklės ir rekomendacijas formuoja tiekėjas. Pirkėjas taisykles integruoja į Zabbix platformą.
4.3. System update		4.3. Sistemos naujinimai
4.3.1.	System operating system updates are performed according to the manufacturer's requirements, but at least three times a year.	Sistemos operacinių sistemų atnaujinimai atliekami pagal gamintojo reikalavimus, bet ne rečiau kaip tris kartus per metus.

4.3.2.	The system's production (PROD) environment must be running the latest stable software version	Sistemos gamybinėje (PROD) aplinkoje turi veikti naujausia stabili programinės įrangos versija.
4.3.3.	Software updates must be performed once during the contract period.	Programinės įrangos versijos naujinimas atliekamas vieną kartą sutarties galiojimo metu.
4.3.4.	The Software version update must be organized no earlier than 9 months before the end of the contract.	Programinės įrangos versijos naujinimas turi būti organizuotas ne anksčiau nei 9 mėnesiai iki sutarties galiojimo pabaigos.
4.3.5.	Updating the system database is subject to identical requirements as updating the system.	Sistemos duomenų bazės naujinimui taikomi identiški reikalavimai kaip ir sistemos naujinimui.
4.3.6.	The Supplier must perform all the necessary configuration work of the system in hardware and software in order to connect the updated system to EVKS and all RTUs.	Tiekėjas turi atlikti visus būtinus sistemos konfigūravimo darbus aparatinėje bei programinėje įrangoje, kad atnaujinama sistema būtų prijungta prie EVKS ir visų TSPJ.
4.3.7.	The Supplier must maintain the exact continuity (concept) of the technical solutions operated and installed by the Buyer, the homogeneity and compatibility of the installed equipment in order to ensure and achieve the maximum functionality of the entire system.	Tiekėjas turi išlaikyti tikslų Pirkėjo eksploatuojamų ir įrenginjamų techninių sprendimų tęstinumą (konceptiją), diegiamos įrangos homogeniškumą, suderinamumą, kad būtų užtikrintas bei pasiektas maksimalus visos sistemos funkcionalumas.
4.3.8.	In case of version replacement and/or upgrade in the system the following shall be ensured: - All stored data shall be relocated to the new database structure; - Data consistency and integrity shall be maintained; - No stored data shall be lost; - Functionality implemented in the system will not be affected.	Sistemos versijos keitimo ir (arba) atnaujinimo atveju turi būti užtikrinta: - visi saugomi duomenys turi būti perkelti į naują duomenų bazės struktūrą; - duomenų nuoseklumas ir vientisumas; - jokie saugomi duomenys nebus prarasti; - sistemoje įdiegtas funkcionalumas nebus paveiktas.
4.3.9.	System should be implemented in such a way that during updates related to architectural components and/or changing the database, it should be possible to migrate all data without purchasing additional services and licenses from the installer and/or system manufacturer.	Sistema turi būti realizuota taip, kad atliekant atnaujinimus, susijusius su architektūriniais komponentais ir (arba) keičiant duomenų bazę, būtų galimybė atlikti visų duomenų migravimą be papildomų paslaugų ir licencijų įsigijimo iš diegėjo ir (arba) sistemos gamintojo.
4.4. Consultations		4.4. Konsultacijos
4.4.1.	The Supplier must provide consultations to the Buyer's responsible persons by telephone or e-mail.	Tiekėjas privalo Pirkėjo atsakingiems asmenims suteikti konsultacijas telefonu arba elektroniniu paštu.
4.4.2.	The Supplier's technical experts provide system configuration services according to the Buyer's pre-agreed requests. The scope of services shall not exceed 50 hours per year.	Tiekėjo techniniai ekspertai suteikia sistemos konfigūravimo paslaugas pagal iš anksto suderintus Pirkėjo prašymus. Paslaugų apimtis ne didesnė nei 50 valandų per metus.
4.5. General Requirements		4.5. Bendrieji reikalavimai
4.5.1.	Data transmitted, stored, managed, processed and controlled by the system, as well as all copies thereof, must be kept and stored only in the data centres designated by LTG.	Sistemos perduodami, saugomi, tvarkomi, apdorojami ir valdomi duomenys, bei visos jų kopijos turi būti laikomos ir saugomos tik LTG nurodytuose duomenų centruose.

4.5.2.	A database replica must be ensured to ensure data accessibility, immutability to malfunctions, and data restoration possibilities.	Turi būti užtikrinta duomenų bazės replikacija, siekiant užtikrinti duomenų prieinamumą, atsparumą gedimams ir atkūrimo galimybes.
4.5.3.	The amount of information processed by system must not be limited by licenses.	Sistemos apdorojamos informacijos apimtys neturi būti ribojamos licencijomis.
4.5.4.	The system must use UTF-8 character encoding in all stages of data storage, processing, and presentation, ensuring correct rendering of the Lithuanian alphabet and characters of other supported languages. The graphical user interface must be multilingual and fully localized in Lithuanian and English. Localization must cover all user-visible text, including menus, buttons, system notifications, error messages, and help information. The system must support language selection at the user level and ensure consistent application of the selected language throughout the entire session.	Sistema turi naudoti UTF-8 simbolių koduotę visose duomenų saugojimo, apdorojimo ir pateikimo grandyse, užtikrindama teisingą lietuviškos abėcėlės ir kitų palaikomų kalbų simbolių atvaizdavimą. Grafinė naudotojo sąsaja turi būti daugiakalbė ir pilnai lokalizuota lietuvių ir anglų kalbomis. Lokalizacija turi apimti visus naudotojui matomus tekstus, įskaitant meniu, mygtukus, sistemos pranešimus, klaidų žinutes ir pagalbos informaciją. Sistema turi palaikyti kalbos pasirinkimą naudotojo lygiu ir užtikrinti nuoseklų kalbos taikymą visos sesijos metu.
4.5.5.	The system must support different time zones and apply Daylight Saving Times changes automatically according to the selected region by ensuring that changing times does not affect the system performance, data precision, and scheduled operations.	Sistema turi palaikyti skirtingas laiko juostas ir automatiškai taikyti žiemos / vasaros laiko (angl. Daylight Saving Time) pokyčius pagal pasirinktą regioną, užtikrinant, kad laiko keitimas neturėtų įtakos sistemos veikimui, duomenų tikslumui ar suplanuotų operacijų vykdymui.
4.5.6.	The system should have the capabilities to change the default user interface language in real time without restarting the system or logging out from it.	Sistema turi užtikrinti galimybę pakeisti naudotojo sąsajos kalbą realiuoju laiku, be būtinybės paleisti sistemą iš naujo ar atsijungti nuo sesijos.
4.5.7.	The system must ensure that all actions performed by the users must be validated against data correctness, and errors are identified, processed in the way understandable to the user without compromising data integrity and system stability.	Sistema turi užtikrinti, kad visi naudotojų atliekami veiksmai būtų tikrinami dėl duomenų korektiškumo, o klaidos būtų identifikuojamos, apdorojamos ir pateikiamos naudotojui suprantamu būdu, nepažeidžiant duomenų vientisumo ir sistemos stabilumo.
4.5.8.	The system must ensure that all error messages presented to the user are clear, understandable, and contextual. Each error message must specify: 1. What happened (the nature of the error); 2. The cause of the error in a form understandable to the user; 3. The specific actions the user should take to continue working or resolve the issue. Error messages must not disclose internal technical system information.	Sistema turi užtikrinti, kad visi naudotojui pateikiami klaidų pranešimai būtų aiškūs, suprantami ir kontekstiniai. Kiekvienas klaidos pranešimas turi nurodyti: 1. kas įvyko (klaidos pobūdį); 2. klaidos priežastį naudotojui suprantama forma; 3. konkrečius veiksmus, kuriuos naudotojas turėtų atlikti, kad galėtų tęsti darbą arba išspręsti problemą. Klaidų pranešimuose neturi būti atskleidžiama vidinė techninė sistemos informacija.
4.5.9.	The system must not be able to automatically fill in the fields containing sensitive and/or confidential information (e.g. username, password) based on the beginning of the entered text.	Sistemoje pagal įvedamo teksto pradžią neturi būti galimybės automatiškai užpildyti jautrių ir / ar konfidencialių informacijos laukų (pvz.: vartotojo vardas, slaptažodis).

4.5.10.	The user must confirm his/her identity in the System with a password.	Sistemoje naudotojas turi patvirtinti savo tapatybę slaptažodžiu.
4.5.11.	Only authenticated users may see the information provided in the system and perform actions.	Sistemoje pateikiamą informaciją gali matyti ir veiksmus atlikti tik autentifikuoti naudotojai.
4.5.12.	The functionality of prerogatives and/or roles must be realized in the system, which ensures the distinction of functions of administrators and users of the system.	Sistemoje turi būti realizuotas privilegijų ir (arba) rolių funkcionalumas, užtikrinantis sistemos naudotojų ir administratorių funkcijų atskyrimą.
4.5.13.	The system shall be recording (logging) and storing for at least 6 months all user (enabled, disabled and deleted) account activities and their content, as well as all user account and privilege/role security changes and their content.	Sistemos įvykių žurnaluose turi būti registruojami ir ne mažiau kaip 6 mėnesius saugomi visų naudotojų (esamų/aktyvių, deaktyvuotų ir ištrintų) visi atlikti veiksmai kartu su veiksmų turiniu (angl. user activity logging), visi naudotojų paskyrų ir privilegijų / rolių keitimo veiksmai kartu su veiksmų turiniu (angl. security change logging).
4.5.14.	The system shall be capable of passing saved logs to Buyer's manages Security Information and Event Management (SIEM) system, and users of the system and support personnel shall not have possibility to alter or delete any log data.	Sistemos turi turėti galimybę perduoti išsaugotų veiksmų/pakeitimų žurnalinius įrašus į Pirkėjo žurnalinių įrašų kaupimo ir analizės (angl. Security information and event management (SIEM)) sistemą, o sistemos naudotojai ir (arba) sistemos priežiūrą vykstantys asmenys neturi galimybių pakeisti arba ištrinti išsaugotų žurnalų įrašų ar jų turinio.
4.5.15.	System logging must support Syslog standard (RFC 5424) which is required for integration with Buyer's logging system.	Sistemos žurnalai turi palaikyti Syslog standartą (RFC 5424), kuris reikalingas integracijai su naudojama žurnalinių įrašų saugojimo sistema.
4.5.16.	Supplier must ensure that only permitted, licensed, and securely supported hardware and software, including its licenses, source code, and security (encryption) keys, and other components, must be used for development and support of the system.	Tiekėjas privalo užtikrinti, kad būtų naudojama tik leistina, licencijuota ir saugiai palaikoma techninė bei programinė įranga, įskaitant jos licencijas, programinį kodą, saugos (šifravimo) raktus ir kitus komponentus, sistemos kūrimui, veikimui ir vystymui.
4.5.17.	System internal (default, built-in) user accounts must be blocked and may only be used in exceptional or system administration cases (e.g. system update or reset).	Sistemos vidinės (default, built-in) naudotojų paskyros turi būti užblokuotos ir galės būti naudojamos tik išskirtiniais arba sistemos administravimo atvejais (pvz. sistemos atnaujinimas ar atstatymas).
4.5.18.	The Supplier must ensure the fulfilment of all its obligations during the system maintenance and support period, even in cases where changes to the system configuration, database structure, or graphical user interface are made at the Buyer's request, provided such changes are agreed upon and documented.	Tiekėjas privalo užtikrinti visų savo įsipareigojimų vykdymą techninio aptarnavimo ir priežiūros laikotarpiu, net ir tuo atveju, kai Pirkėjo prašymu atliekami sistemos konfigūracijos, duomenų bazės struktūros ar grafinės naudotojo sąsajos pakeitimai, jeigu tokie pakeitimai yra suderinti ir dokumentuoti.
4.5.19.	Supplier shall maintain and provide support to all system software parts till technical support period expiration.	Tiekėjas privalo prižiūrėti ir teikti palaikymą visoms sistemos programinės įrangos dalims iki techninio palaikymo laikotarpio pabaigos.
4.5.20.	Technical support for the software must be provided for all software included in the contract, regardless of its origin – including components developed by the	Programinės įrangos techninis palaikymas turi būti teikiamas visai programinei įrangai, įtrauktai į sutartį, nepriklausomai nuo jos kilmės –

	Supplier, original manufacturer's (OEM) solutions, and third-party software. The Supplier must ensure coordination of support and act as the primary contact.	ties Tiekėjo sukurtiems komponentams, ties originalaus gamintojo (OEM) sprendimams, ties trečiųjų šalių programinei įrangai. Tiekėjas privalo užtikrinti palaikymo koordinavimą ir veikti kaip pagrindinis kontaktinis asmuo.
4.5.21.	Supplier and/or the software suppliers shall notice the Buyer of their intent to discontinue the supply of technical support services, at least 6 months in advance.	Tiekėjas ir (arba) programinės įrangos tiekėjai privalo pranešti Pirkėjui apie savo ketinimą nutraukti techninės pagalbos paslaugų teikimą ne vėliau kaip prieš 6 mėnesius.
4.5.22.	The Supplier must designate a responsible consultant(s) for maintenance. The responsible consultant must supervise the organization of maintenance services, SLA monitoring, and reporting.	Tiekėjas turi paskirti dedikuotą atsakingą konsultantą (-us) priežiūrai. Atsakingas konsultantas turi būti atsakingas už priežiūros paslaugų organizavimą, SLA stebėjimą ir ataskaitų teikimą.
4.5.23.	During the provision of services, the Supplier must ensure that the Supplier, the equipment the Supplier supplies, and other economic entities the Supplier uses (economic entities whose capacities are relied upon for qualification purposes, subcontractors, etc.) comply with the cybersecurity requirements for essential cyber security subjects set out in the Cyber Security Requirements Description (hereinafter referred to as the Description) approved by Resolution No. 818 of the Government of the Republic of Lithuania of 13 August 2018 "On the Implementation of the Law on Cyber Security of the Republic of Lithuania". At the request of the Buyer, within a period agreed by both parties, the Supplier must provide explanations and/or other evidence (e.g., certificates and/or policies, and/or process descriptions, and/or external audit conclusions) confirming that the Supplier will ensure compliance with the requirements of the Description.	Tiekėjas paslaugų teikimo metu privalo užtikrinti, kad jis, jo tiekiama įranga ir jo pasitelkiami kiti ūkio subjektai (ūkio subjektai, kurių pajėgumais remiamasi kvalifikacijai pagrįsti, subtiekejai ir kita) atitinka Lietuvos Respublikos Vyriausybės 2018-08-13 nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ patvirtintame Kibernetinio saugumo reikalavimų apraše (toliau – Aprašas) esminiams kibernetinio saugumo subjektams nustatytus kibernetinio saugumo reikalavimus. Perkančiajai organizacijai paprašius, per abiejų šalių suderintą terminą, Tiekėjas privalo pateikti paaiškinimus ir (ar) kitus įrodymus (pvz., sertifikatus ir (ar) politikas, ir (ar) procesų aprašus, ir (ar) išorinio audito išvadas), kurie patvirtintų, kad Tiekėjas užtikrins atitiktį Aprašo reikalavimams.
4.5.24.	The Supplier shall make it possible for the Buyer or its authorized parties to perform own audit/verification of the system development and support arrangements at least once per calendar year or in the event of a major cyber incident (in accordance with the provisions of the Cybersecurity Law) in order to evaluate the organizational and technical measures of protection of Buyer's Data.	Tiekėjas turi užtikrinti galimybę Pirkėjui ar jo įgaliotam partneriui ne rečiau kaip vieną kartą per metus arba įvykus dideliam (pagal Kibernetinio saugumo įstatymo nuostatas) kibernetiniam incidentui atlikti sistemos palaikymo ir vystymo veiklos auditą ar patikrą, siekiant įvertinti taikomas Pirkėjo duomenų saugos užtikrinimo organizacines bei technines priemones.
4.5.25.	If, during the provision of services, the Supplier needs to obtain the Buyer's non-public information (internal information, confidential information or commercial (trade) secrets), an information transfer agreement must be signed. This agreement must specify: - the information to be transferred and its confidentiality level; - the recipients of the information; - the method of information transfer;	Jei paslaugų teikimo metu Tiekėjui reikalinga gauti Pirkėjo neskelbtinos informacijos (vidinės informacijos, konfidencialios informacijos ar komercinių (gamybinių) paslapčių) turi būti pasirašomas informacijos perdavimo susitarimas. Šiame susitarime turi būti nurodyta: - perduotina informacija ir jos konfidencialumo lygis; - informacijos gavėjai; - informacijos perdavimo būdas;

	- technical and organizational information security requirements that the Supplier must ensure when protecting the Buyer's non-public information.	- techniniai ir organizaciniai informacijos saugumo reikalavimai, kuriuos turi užtikrinti Tiekėjas, apsaugodamas neskelbtiną Pirkėjo informaciją.
4.5.26.	Buyer shall be notified immediately about system's information and cyber security events and incidents or personal data breach, as well as their implication on Buyer's information and data protection and remediation status. Within 24 hours, an early warning should be communicated, as well as some first presumptions regarding the kind of incident to the LTG digital security team or competent authority. After 72 hours, a full notification report must be communicated, containing the assessment of the incident, severity and impact and indicators of compromise. After 1 month, a final report must be communicated. Buyer shall have possibility to liaise with security event and incident management personnel to get assurance about the remediation process efficiency.	Pirkėjas turi būti nedelsiant informuojamas apie sistemos informacijos ir kibernetinės saugos įvykius ir incidentus ar asmens duomenų saugumo pažeidimus, jų įtaką Pirkėjo informacijos ir duomenų saugumui bei jų valdymo būklę. Per 24 valandas LTG skaitmeninio saugumo komandai arba kompetentingai institucijai turėtų būti perduotas išankstinis įspėjimas ir keletas pirmųjų prielaidų apie incidento pobūdį. Po 72 valandų turi būti perduota išsami pranešimo ataskaita, kurioje pateikiamas incidento įvertinimas, sunkumas ir poveikis bei kompromitavimo rodikliai. Po 1 mėnesio turi būti pateikta galutinė ataskaita. Pirkėjas turi turėti galimybę susisiekti su saugos įvykius ir incidentus valdančiais asmenimis, kad įsitikinti valdymo proceso efektyvumu.
4.5.27.	The Supplier shall ensure that requirements are applied to its partners, subcontractors, system developers and/or other Parties involved in production, support and development of the system.	Tiekėjas privalo užtikrinti, kad nurodyti reikalavimai būtų taikomi jo partneriams, subrangovams, sistemos gamintojams ir (arba) kitoms Šalims, dalyvaujančioms sistemos kūrimo, vystymo ir palaikymo veikloje.
4.5.28.	The system must ensure that all stored data is authentic, immutable, and consistent — meaning it is protected from unauthorized modification, loss, or corruption, while guaranteeing the reliability of its origin, logical consistency, and technical integrity throughout its entire lifecycle.	Sistema turi užtikrinti, kad visi saugomi duomenys būtų autentiški, nekintami ir vientisi - t. y. apsaugoti nuo neautorizuoto pakeitimo, praradimo ar sugadinimo, užtikrinant jų kilmės patikimumą, loginį nuoseklumą ir techninį integralumą viso gyvavimo ciklo metu.
4.5.29.	The system must ensure the ability to manage user roles and their access rights. It must be possible to: 1. Assign, modify, and remove user roles; 2. Assign, change, and delete access rights lists assigned to roles (e.g., access to functions, data, or modules).	Sistema turi užtikrinti galimybę administruoti naudotojų roles ir jų prieigos teises. Turi būti galima: 1. Priskirti, modifikuoti ir panaikinti naudotojų roles; 2. Priskirti, keisti ir ištrinti rolėms priskirtus prieigos teisių sąrašus (pvz., funkcijų, duomenų ar modulių pasiekiamumą).
5. DOCUMENTS PROVIDED DURING THE PERFORMANCE OF THE CONTRACT		5. SUTARTIES VYKDYMO METU TEIKIAMAI DOKUMENTAI
5.1.	The supplier shall provide a report on the services provided and the technical problems/deviations registered and resolved at agreed intervals. Provided in electronic form, in Lithuanian or English, during the performance of the contract.	Tiekėjas teikia suteiktų paslaugų bei registruotų ir išspręstų techninių problemų/pašalintų nukrypimų ataskaitą suderintu periodiškumu. Teikiama elektronine forma, lietuvių arba anglų kalba, sutarties vykdymo metu.
5.2.	The supplier provides detailed recommendations for updating operating systems. Provided in electronic form, in Lithuanian or English, during the performance of the contract.	Tiekėjas pateikia išsamias rekomendacijas, kaip atnaujinti operacines sistemas. Teikiama elektronine forma, lietuvių arba anglų kalba, sutarties vykdymo metu.

5.3.	The supplier provides detailed recommendations for updating the system (including the database). Provided in electronic form, in Lithuanian or English, during the performance of the contract.	Tiekėjas pateikia išsamias rekomendacijas sistemos (įskaitant duomenų bazę) atnaujinimui. Teikiama elektronine forma, lietuvių arba anglų kalba, sutarties vykdymo metu.
5.4.	A system performance report including primary performance rates should be generated each calendar month. The report must be sent to System owner and/or authorized contact person using electronic means mutually agreed in advance. Provided in electronic form, in Lithuanian or English, during the performance of the contract.	Kiekvieną kalendorinį mėnesį turi būti automatiškai generuojama Sistemos veikimo ataskaita, apimanti pagrindinius veikimo rodiklius. Ataskaita turi būti pateikiama Pirkėjui ir (arba) oficialiai paskirtam kontaktiniam asmeniui elektroniniu būdu. Teikiama elektronine forma, lietuvių arba anglų kalba, sutarties vykdymo metu.
5.5.	Supplier shall provide the Buyer with helpdesk contacts. Helpdesk shall include following means of contact: * On-call support; * Web forms; * Email. Provided in electronic form, in Lithuanian or English, during the performance of the contract.	Tiekėjas turi pateikti Pirkėjui pagalbos tarnybos kontaktus. Pagalbos tarnyba turi apimti šiuos susisieikimo būdus: * On-call palaikymas; * Interneto formos; * El. paštas. Teikiama elektronine forma, lietuvių arba anglų kalba, sutarties vykdymo metu.
5.6.	the Supplier must generate and submit a Software Bill of Material (SBOM) report for system components: in a CyclonDX standard JSON format file with integrity verification. After updating the system, a new SBOM report must be generated and submitted. Provided in electronic form, in Lithuanian or English, during the performance of the contract.	Tiekėjas privalo sugeneruoti ir pateikti sistemos komponentų (angl. Software Bill of Material, SBOM) ataskaitą: CyclonDX standarto JSON formato faile su vientisumo patikra (angl. integrity verification). Atnaujinus sistemą, turi būti sugeneruota ir pateikta nauja SBOM ataskaita. Teikiama elektronine forma, lietuvių arba anglų kalba, sutarties vykdymo metu.
5.7.	Compliance with cybersecurity requirements pursuant to Resolution No. 818 of the Government of the Republic of Lithuania of 13 August 2018. Provided in electronic form, in Lithuanian or English, during the performance of the contract.	Atitiktis kibernetinio saugumo reikalavimams dėl Lietuvos Respublikos Vyriausybės 2018-08-13 nutarimo Nr. 818. Teikiama elektronine forma, lietuvių arba anglų kalba, sutarties vykdymo metu.
5.8.	The Supplier must provide a Service Acceptance–Transfer Act. In the acceptance–transfer act, the Supplier shall list in detail the services performed. It is submitted at the time of contract performance, after the Service has been completed.	Tiekėjas turi pateikti Paslaugų priėmimo – perdavimo aktą. Tiekėjas priėmimo – perdavimo akte išsamiai išvardina atliktas paslaugas. Teikiamas sutarties vykdymo momentu, atlikus Paslaugą.
FULFILLMENT OF OBLIGATIONS		PRIEVOLIŲ VYKDYMAS
6. SERVICE PROCEDURE		6. PASLAUGŲ TEIKIMO TVARKA
6.1.	The buyer will use the incident management system ServiceNow to manage system outages. The buyer will notify the supplier by phone when the system outage is critical. Additional communication may be via email, phone, or Teams.	Sistemos sutrikimų valdymui pirkėjas naudosis incidentų valdymo sistema ServiceNow.

6.2.	The Supplier will not be granted direct access to the Customer's incident management system. The Supplier must have its own incident management system. The Supplier must have a permanently operating technical support centre (help desk) that provides primary assistance with software operation issues.	Tiekėjui nebus suteiktos tiesioginės prieigos prie Pirkėjo incidentų valdymo sistemos. Tiekėjas privalo turėti savo incidentų valdymo sistemą. Tiekėjas privalo turėti nuolat veikiantį techninės pagalbos centrą (pagalbos tarnybą), kuriame teikiama pirminė pagalba programinės įrangos veikimo klausimais.
6.3.	Primary communication about system outages will be handled through integration between buyer and supplier incident management tools. The integration mechanism are agreed upon after the contract is signed. Additional communication may be handled via email, phone, or Microsoft Teams. Buyer notifies supplier by phone when system outage is critical.	Pagrindinė komunikacija apie sistemos sutrikimus bus vykdoma per integraciją tarp pirkėjo ir tiekėjo incidentų valdymo įrankius. Integracijos mechanizmas suderinamas po sutarties pasirašymo. Papildoma komunikacija gali būti vykdoma El. paštu, telefonu arba Microsoft Teams platforma. Pirkėjas informuoja telefonu tiekėją kai sistemos sutrikimas yra kritinis.
6.4.	The criticality of faults is selected by the L1 and L2 responsibility level support team, but the criticality can be discussed and changed at higher levels	Sutrikimų kritiškumą parenka L1 ir L2 atsakomybės lygio pagalbos grupė, tačiau kritiškumas gali būti aptartas ir pakeistas aukštesniuose lygiuose
6.5.	In the event of a critical incident, within 10 working days after the incident has been resolved, the supplier must provide a report on the causes of the incident and the resolution, as well as a description and timeline for the preventive measures that will be implemented.	Kritinio incidento atveju, per 10 darbo dienų po incidento išsprendimo, tiekėjas turi pateikti incidento priežasčių ir sprendimo ataskaitą, bei prevencinių priemonių, kurios bus įgyvendintos, aprašymą bei terminus.
6.6	The deadline set for eliminating system malfunctions may be extended by written agreement between the Supplier and the Buyer if delays, obstacles or disruptions occur, the occurrence of which the Supplier has no influence on and is not liable for these delays, obstacles or disruptions, and these specified actions can be reasonably attributed to the actions or inaction of third parties	Sistemos sutrikimų šalinimui nustatytas terminas gali būti pratęstas Tiekėjo ir Pirkėjo rašytiniu susitarimu, jeigu atsiranda uždelsimų, kliūčių ar trukdymų, kurių atsiradimui Tiekėjas neturi įtakos ir už šiuos uždelsimus, kliūtis ar trukdymus jis neatsako, ir šie nurodyti veiksmai pagrįstai priskirtini trečiųjų asmenų veiksams ar neveikimui.
6.7.	The deadline set for eliminating system malfunctions may be extended by written agreement between the Supplier and the Buyer if there is a change or repeal of legal acts that affect the performance of contractual obligations, or if new legal acts come into force and the Supplier cannot objectively influence this.	Sistemos sutrikimų šalinimui nustatytas terminas gali būti pratęstas Tiekėjo ir Pirkėjo rašytiniu susitarimu, jeigu atsiranda teisės aktų, kurie turi įtakos sutartinių prievolių vykdymui, pasikeitimas, panaikinimas, naujų teisių aktų įsigaliojimas ir Tiekėjas objektyviai negali tam daryti įtakos
6.8.	System malfunction is considered resolved if the Buyer does not submit a claim to the Supplier within 5 (five) business days of the Buyer.	Sistemos sutrikimas laikomas pašalintu, jeigu per 5 (penkias) Pirkėjo darbo dienas Pirkėjas nepateikia Tiekėjui pretenzijos.
6.9.	The Supplier must represent the Buyer in resolving all system incidents related to third-party software and act as a single contact, coordinating communication, analysis, and resolution processes with third parties until the incident is fully resolved or a justified explanation is provided.	Tiekėjas privalo atstovauti Pirkėjui sprendžiant visus sistemos incidentus, susijusius su trečiųjų šalių programine įranga, ir veikti kaip vienas kontaktinis asmuo, koordinuojantis komunikaciją, analizę ir sprendimo eigą su trečiosiomis šalimis, iki visiško incidento išsprendimo arba pagrįsto paaiškinimo pateikimo.

6.10	The system's technical support must be provided directly by the Supplier, or in cooperation with the original software supplier, or both together, ensuring uninterrupted support and prompt incident resolution throughout the entire support period.	Sistemos techninę pagalbą privalo teikti Tiekėjas tiesiogiai, arba bendradarbiaujant su programinės įrangos originaliu tiekėju, arba abu kartu, užtikrinant nenutrūkstamą palaikymą ir operatyvų incidentų sprendimą viso palaikymo laikotarpio metu.
6.11.	The Buyer shall prepare and periodically update a system recovery plan, which shall include regular data backups and data and service recovery procedures. The Supplier shall provide guidance and participate in the system recovery process. System recovery shall be performed once a year.	Pirkėjas rengia ir periodiškai naujina sistemos atkūrimo planą, kuris apima reguliariai atliekamą atsarginių duomenų kopijų kūrimą bei duomenų ir paslaugų atstatymo procedūras. Tiekėjas teikia rekomendacijas ir dalyvauja sistemos atstatymo procese. Sistemos atstatymas vykdomas kartą per metus.
6.12	The Supplier is not entitled, during the performance of the Contract, to provide services that do not comply with the requirements of the Procurement Documents and/or services whose provision is restricted due to international sanctions (as understood in the Law of the Republic of Lithuania on the Implementation of International Sanctions) and/or due to threats to national security, as defined in the Procurement Documents and in the Law on Public Procurement of the Republic of Lithuania / the Law on Procurement in the Fields of Water Management, Energy, Transport and Postal Services.	Tiekėjas neturi teisės Sutarties vykdymo metu teikti paslaugų, kurios neatitinka Pirkimo dokumentų reikalavimų ir (ar) kurių teikimas yra apribotas dėl tarptautinių sankcijų (kaip jos suprantamos LR tarptautinių sankcijų įstatyme) ir (ar) dėl jų grėsmės nacionaliniam saugumui, kaip tai apibrėžta Pirkimo dokumentuose ir LR viešųjų pirkimų įstatyme / LR pirkimų, atliekamų vandentvarkos, energetikos, transporto ir pašto paslaugų srities perkančiųjų subjektų, įstatyme.

7. MATRIX OF RESPONSIBILITIES

	Buyer	Supplier
Software licences		
Operating system licences	X	
Database licences		X
GE SCADA application licences	X	
Server infrastructure		
Hardware configuration	X	
Hardware and VM licences	X	
Backup VMs	X	
Backup DB mechanism		X
DB backup storage	X	
Hardware and VM monitoring	X	
OS patching	X	
OS patching plan		X
Network infrastructure		
Configuration of the network equipment	X	
Configuration of the firewall rules	X	
Provision of remote access	X	

7. ATSAKOMYBIŲ MATRICA

	Pirkėjas	Tiekėjas
Programinės įrangos licencijos		
Operacinės sistemos licencijos	X	
Duomenų bazės licencijos		X
GE SCADA aplikacijos licencijos	X	
Serverių infrastruktūra		
Aparatinės įrangos konfigūravimas	X	
Aparatinės įrangos ir VM licencijos	X	
Atsarginės kopijos VM	X	
Atsarginės kopijos DB mechanizmas		X
Atsarginės DB kopijos saugojimas	X	
Aparatinės dalies ir VM monitoringas	X	
OS naujinimas	X	
OS naujinimo planas		X
Tinklų infrastruktūra		
Tinklo įrangos konfigūravimas	X	
Ugniasienės taisyklių konfigūravimas	X	
Nuotolinės prieigos suteikimas	X	

Application			Aplikacija		
Application configuration		X	Aplikacijos konfigūracija		X
Application and DB monitoring	X	X	Aplikacijos ir DB monitoringas	X	X
Application and DB monitoring plan		X	Aplikacijos ir DB monitoringo planas		X
Installation of the application on users' PCs	X		Aplikacijos diegimas naudotojų PC	X	
Application and DB patch		X	Aplikacijų ir DB naujinimas		X
System support levels			Sistemos palaikymo lygiai		
L1	X		L1	X	
L2	X		L2	X	
L3	X		L3	X	
L4		X	L4		X
System recovery plan			Sistemos atstatymo planas		
Preparing a plan	X		Plano rengimas	X	
Recommendations		X	Rekomendacijos		X
Implementing the recovery plan	X	X	Atstatymo plano vykdymas	X	X
8. ATTACHMENTS			8. PRIEDAI		
Annex No. 1 – Environmental (Green) Criteria. Annex 2. NFR (non-functional) requirements for information security and GDPR.			Priedas Nr. 1 – Aplinkos apsaugos (žalieji) kriterijai 2 priedas – NFR (nefunkciniai) reikalavimai informacijos saugai ir BDAR.		