#	Reikalavimas	Requirement	Cloud ar On Premise, Hybrid	Reikalavimo tipas / Requirement category	Privaloma (mandatory) / Neprivaloma (optional)	Prioritetas Aukštas (High) / Vidutinis (Medium) / Mažas (Low)	Reikalavimo įgyvendinimas Sistemoje (Įgyvendintas, Bus įgyvendintas, Nebus įgyvendintas) / The implementation of a requirement in the System (Implemented, Will be implemented, Will not be	Comments	INDRA comment (27/10/2021)
NFR-001	Bendro sistemos aprašymo dokumentas turi apimti: * sistemos tikslą * aprašyti sistemos funkcijas * pateikti aukšto lygio sistemos architektūrą	General description of the system document must contain: * must explain system purpose * must describe system functions * must present high level system architecture	All	Dokumentavimas/ Documentation	Privaloma (mandatory)	Vidutinis (Medium)	Bus įgyvendintas (Will be implemented)		During the design phase will be provided a General description of the system
NFR-002	Tipinis duomenų bazės atsakymo laikas iki 0.01s. Maksimalus atsakymo laikas 0.05 s. Pateikite ilgiausią / vidutinį laiką kaip etalonus, kad galėtume išbandyti sistemą.	Typical database response time up to 0.01s. Maximum response time 0.05 s. Please provide longest/average time as benchmarks for us to test system against.	All	Duomenų archyvavimas/ Data archive	Privaloma (mandatory)	Aukštas (High)	Nejgyvendintas (Will not be implemented)		The Postgresql database is delivered fully optimized. Out of Scope. Optimization of the querys are out of scope. After sign the contract and at the begining of the project, Indra can get a report in order to know the current top 10 heavy queries of each database and each response time. This response time can be set as the minimum level to comply after the migration It is important to note, that after the migration from Oracle to Postgrest this top 10 could not be the same.
NFR-003	Duomenų bazė turi automatiškai generuoti 24 val replikas ir jas iškelti į atitinkamą vietą tinkle. Peteikite detalią architektūrą su aprašymu.		All	Duomenų archyvavimas/ Data archive	Privaloma (mandatory)	Aukštas (High)	Bus įgyvendintas (Will be implemented)		Indra proposes the implementation of a Postgresql system in HA using Streaming Replication technology (native to postgresql), for which there will be a master and a slave database (with read-only access and replicated asynchronously).
NFR-004	Aktyviomis replikomis laikomos duomenų bazės replikos, kurios yra laikomos iki 14 d. Vėliau tokios replikos privalo būti iškeltos iš aktyvios serverio aplinkos į archyvavimo aplinką. Šios aplinkos negalim būti vienoje mašinoje	Database replicas that are stored until 14 days are considered active replicas. Such replicas must then be retrieved from the active server environment to the archiving environment. This environment cannot be on the same machine	All	Duomenų archyvavimas/ Data archive	Privaloma (mandatory)	Aukštas (High)	Bus įgyvendintas (Will be implemented)		The replication that will be carried out through Streaming Replication will always be active since it will form part of the high availability system proposed by Indra
NFR-005	Turi būti galimybė patikrinti duomenų bazėje saugomus duomenis, jų neprieštaringumą ir išsamumą;	It must be possible to verify the data stored in the database, their consistency and completeness	All	Duomenų archyvavimas/ Data archive	Neprivaloma (optional)	Aukštas (High)	Bus įgyvendintas (Will be implemented)		The database manager guarantees the integrity of the data, even so, it can be verified through queries and tools such as pgcheck
NFR-006	Turi būti galimybė plėsti duomenų bazę, perkelti ją į kitą vietą ir esant reikalui, atlikti atstatymą iš kopijų;	It must be possible to expand the database, relocate it and, if necessary, restore from copies	All	Duomenų archyvavimas/ Data archive	Privaloma (mandatory)	Aukštas (High)	Bus įgyvendintas (Will be implemented)		Postgresql can grow by tablespaces, it can grow both horizontally and vertically. Restorations can be made with both a physical backup and a logical backup
NFR-007	Duomenų atsarginės kopijos atlikimo procedūrų metu turi būti tenkinami Sistemos greitaveikai keliami reikalavimai.	System performance requirements shall be met during data backup procedures.	All	Pasiekiamumas ir patikimumas/ Availability and Reliability	Privaloma (mandatory)	Aukštas (High)	Bus įgyvendintas (Will be implemented)		During the backup processes, performance is ensured and for this, off-peak hours will be sought to perform them.
NFR-008	Įvykus incidentui, prarandant dalinę infrastruktūrą (pvz. vieną iš fizinių stočių), sistemos greitaveika neturi nukentėti. T.y. bendras/sumarinis sistemos resursų skaičius turi būti rezervuotas ir sugebėti apdoroti dalinį infrastruktūros praradimą.	In case of incident, loosing part of infrastructure (e.g. one of physical nodes), overall system performance can't degrade. Total system resources must be reserved for partial loosing of system IT infrastructure.	All	Infrastruktūra/Infrastructure	Privaloma (mandatory)	Aukštas (High)	Bus įgyvendintas (Will be implemented)		Indra proposes a database architecture in high availability, so that the performance of the database system and availability is guaranteed.
NFR-009	Įvykus incidentui, prarandant ryšį tarp dubliuojančių sistemos elementų, neturi kilti situacija, kai kiekviena iš dubliuojančių dalių dirbą savarankiškai, pažeidžiant bendrą duomenų integralumą (angl. cluster brain split.)	In case of loosing communication between duplicate elemnents of the system, individual parts of the system can't take master role at same time (cluster brain split). This event can't lead to breaking data integrity.	All	Infrastruktūra/Infrastructure	Privaloma (mandatory)	Žemas (Low)	Bus įgyvendintas (Will be implemented)		To avoid the split brain, a 3 pgppol will be implemented in an independent virtual server that will act as a tiebreaker if necessary.
NFR-010	Įvykus incidentui, dėl kurio Sistemos programinė įranga perleidžiama iš naujo (pvz., elektros energijos tiekimo sutrikimas, kt.), programinės įrangos paleidimas turi įvykti automatiškai be žmogaus įsikišimo, negali dingti į Sistema suvesti ir incidento metu apdorojami duomenys ar programinės įrangos konfigūracijos duomenys (reikalavimas negalioja portalų / paskyrų užpildymo laukuose įvestiems, bet incidento metu dar neišsaugotiems duomenims).	In case of incident causing System restart (such as loss of the power), software shall be restarted automatically without human interference. Data entered into the System and processed during the incident, as well as, software configuration data shall not be lost. This requirement is not applied for data entered GUI, but not saved before the incident.	All	Pasiekiamumas ir patikimumas/ Availability and Reliability	Neprivaloma (optional)	Aukštas (High)	Bus įgyvendintas (Will be implemented)		At the database level, since everything is on the same network, the change from master node to standby, in case of master failure, will be done automatically. This will be done thanks to the pgpool, which is the component that monitors the status of the database members.
NFR-011	Turi būti pateikta vartotojo dokumentacija: * Mokomoji medžiaga * Sistemos testavimo scenarijai * Naudotojo vadovas (kiekvienai rolei)	Such documentation from users point of view must be provided: * Training material * System testing scenarios * User guide (for each role)	All	Dokumentavimas/ Documentation	Neprivaloma (optional)	Žemas (Low)	Bus įgyvendintas (Will be implemented)		During the project phase, accodiring with the agreed scheudule, will be provided this documentation

NFR-012	Sistemos kūrimo, palaikymo ir vystymo veikloje turi būti įgyvendintos organizacinės ir techninės saugumo valdymo priemonės, atitinkančios ISO27000 šeimos ir (arba) lygiaverčių standartų reikalavimus. Šių priemonių įgyvendinimas turi būti patvirtintas reguliarių vidinių ir (arba) išorinių patikrų rezultatais ir sertifikatais, įskaitant bet ne apsiribojant SOC 2 ir SSAE 16 ataskaitomis. Tiekėjas turi pateikti atitiktį patvirtinančią dokumentaciją (pvz. sertifikatus ar ataskaitas) Pirkėjui.	For the System production, support and development, organizational and technical security management measures shall be implemented as specified in ISO27000 family and/or equivalent standards and requirements. The implementation of such measures shall be proven via regular internal and/or external audits and certifications, including but not limited to SOC 2 and SSAE 16 reports. The Supplier shall provide documented conformity statements (e.g. certificates or reports) about compliance with abovementioned requirements to the Customer.	All	Saugumas ir žurnalizavimas/ Security and logging	Privaloma (mandatory)	Aukštas (High)	Įgyvendintas (Implemented)	LTG:turi būti paliktas.Tiekejas pateiks kopija turimo ISO certifikato (bendras ISO kuri INDRA jau turi) per CVPIS kaip viena iš priedu, prie pasiulymo	Limited to submit Indra GENERAL Certification ISO 27001 to level company, not specific for this project
NFR-013	Sistemos kūrimui ir vystymui turi būti taikomi griežti programinės įrangos kūrimo gyvavimo ciklo (SDLC) metodai. SDLC metodai apima geriausią praktiką ir standartinius reikalavimus saugiam programinės įrangos (kodo) kūrimui ir nuolatiniam tikrinimui, įskaitant pažeidžiamumo vertinimus ir testavimą nepalankiausiomis sąlygomis. Tiekėjas turi pateikti SDLC metodų naudojimą patvirtinančią dokumentaciją Pirkėjui.	For the system development, rigid Software Development Lifecycle (SDLC) methods shall be used. SDLC methods shall include best practices and standard requirements for secure software (code) development and continuous verification, including vulnerability assessments and stress testing. The Supplier shall provide documented evidence of implementation of SDLC methods to the Customer.	All	Saugumas ir žurnalizavimas/ Security and logging	Privaloma (mandatory)	Aukštas (High)	Įgyvendintas (Implemented)	LTG: Tai turi būti vidaus dokumentas, kuriame tiekejas deklaruoja, kad vykdo SDLC metodus - turi pateikti veiklos aprasymą; Indra: in general agree, will check internally. Užtenka Indros deklaracijos.	Limited to submit the INDRA internal methods to validate projects
NFR-014	Tiekėjas privalo užtikrinti, kad visa migravimo darbams atlikti reikalinga aparatinė ir programinė įranga, įskaitant licencijas, programinį kodą, saugos (šifravimo) raktus ir kt., jei tokia bus naudojami, yra valdoma ir kontroliuojama, užtikrinant, kad Sistemos palaikymui ir vystymui būtų naudojama tik leistina ir licencijuota aparatinė ir programinė įranga pagal SIL-2 sertifikatą.	The Supplier shall ensure that all hardware and software components, including equipment, licenses, code, security (encryption) keys and etc., if such be required for migration purposes, are fully managed and controlled to ensure that only permitted and licensed hardware and software is used for System development and support, according to SIL-2 certificate.	All	Saugumas ir žurnalizavimas/ Security and logging	Privaloma (mandatory)	Aukštas (High)	Įgyvendintas (Implemented)	LTG: Migruota sistema tures toki pat sertifikata kaip dabar - tiekejas turi tai uztikrinti. Indra: adapt text to procurement object - no hardvare, no new davinci modules; SIL-2 only for critical commands, specific functionalities, does not cover licences, neither hardvare. Licences of software should be compatible with SIL2...etc	Indra understand that SIL-2 certificate applies only for the current SIL-2 certified modules of the CTC App. Indra understand that only If code related to these modules changes, it must be approved again to SIL2. Therefore, in the scope of the migration project in is not included approve again to SIL2 the current certified modules of the CTC App due to it is not contemplated change them Indra will provide a document (SRAC Fulfillment) to certificate that SIL-2 certificated modules has not been affected by this project
NFR-015	Sistemoje neturi būti įkoduotų (*angl. Hard Coded*) duomenų, kuriems koreguoti ir / ar keisti būtų reikalingos diegėjo paslaugos.	The system shall not have Hard Coded data, which correction and/or modification require additional vendor services.	All	Sistemos architektūra/ Technology Architecture	Neprivaloma (optional)	Aukštas (High)	Įgyvendintas (Implemented)		Already implmented
NFR-016	Jeigu daromi su eismo sauga susiję programinio kodo pakeitimai, jie turi būti resertifikuoti SIL2.	If code changes related to trafic safety are implemented, it must be approved by SIL2.	All	Sistemos architektūra/ Technology Architecture	Privaloma (mandatory)	Aukštas (High)	Įgyvendintas (Implemented)		Indra understand that SIL-2 certificate applies only for the current SIL-2 certified modules of the CTC App. Indra understand that only If code related to these modules changes, it must be approved again to SIL2. Therefore, in the scope of the migration project in is not included approve again to SIL2 the current certified modules of the CTC App due to it is not contemplated change them Indra will provide a document (SRAC Fulfillment) to certificate that SIL-2 certificated modules has not been affected by this project
NFR-017	Prieš įdiegiant Sistemą į darbinę aplinką ir užkeliant Pirkėjo duomenis, Tiekėjas turi pateikti dokumentus įrodančius, 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 įrankiu, įvertintu nepriklausomų šalių, t.k. Gartner, Forrester ar kt.	Before deploying the System to the production environment (a.k.a. going live) and uploading Customer Data, the Supplier shall provide the Customer with the documents, confirming that system do not have critical, high and medium level cyber security vulnerabilities, identified via vulnerability assessment performed by NKSC or using one of the TOP 10 rated vulnerability assessment tools, rated by independent parties, such as Gartner, Forrester, etc.	All	Saugos valdymas/Security governance	Privaloma (mandatory)	Aukštas (High)	Bus įgyvendintas (Will be implemented)	LTG:naujas/ IndraI: will share with Indra security manager internally and revert on it	The security assessments included as part of the migration Project are a system vulnerability assessment and a hardening audit. The objective of these security processes is to reduce the risk surface of systems before deployment. This approach ensures that all critical vulnerabilities are resolved and a secure configuration is applied in the IT platform. The result of these processes will be included in a Vulnerability and Hardening Audit report that will be delivered to LTG as evidence of the vulnerabilities resolved and the secure configuration applied.