**TECHNINĖ SPECIFIKACIJA**

1. **SĄVOKOS IR SUTRUMPINIMAI**

|  |  |
| --- | --- |
| **Naudojamos sąvokos** | **Aprašymas** |
| **Incidentas** | Paslaugos teikimo sutrikimas, dėl kurio paslauga tampa iš dalies nepasiekiama Užsakovui arba sutrinka bent viena iš paslaugos funkcijų. |
| **IT paslaugų valdymo (ITSM) platforma** | Tiekėjo pasiūlyta klaidų ir vystymo paslaugų registravimo platforma. |
| **Keitimas** | Paslaugos konfigūracijos elemento, proceso ar dokumento ir kt., kas gali įtakoti paslaugos teikimą, papildymas, pakeitimas ar pašalinimas. |
| **Klaida** | Sistemos veikimo, dokumentacijos neatitikimas aprašytai specifikacijai, sistemos sutrikimai dėl netinkamų technologinių sprendimų, neigiama susijusių standartinių komponentų įtaka sistemos veikimui, netinkamas specifinių programinių priemonių panaudojimas, kiti programiniai bei technologiniai faktoriai, darantys neigiamą įtaką sistemos darbui. |
| **Kokybės garantija / Garantija / Garantinis aptarnavimas** | Sutarties galiojimo metu aptiktų klaidų / neatitikimų sutartiniams įsipareigojimams šalinimas Tiekėjo sąskaita. |
| **Kritinė klaida** | Nustatyta klaida ir (ar) problema, dėl kurios naudotojas negali vykdyti numatytų būtinų funkcijų (negali prisijungti prie Sistemos; neveikia pagrindinės Sistemos funkcijos (nėra galimybės teikti prašymus sutikimui ar leidimui gauti, negalima valdyti Kliento prašymų, išduotų sutikimų bei leidimų vykdyti darbus, Sistema veikia ne taip kaip numatyta techninėje specifikacijoje, sistemos dokumentuose, teisės aktuose ar kituose susijusiuose dokumentuose ir pan.); Sistema veikia lėtai / nestabiliai ir pan.) ir nežinomas joks kitas alternatyvus šios funkcijos vykdymas. |
| **Naudotojas** | Užsakovo darbuotojas arba Užsakovo Klientas, naudojantis Sistemos aplikaciją bei Kliento portalą. |
| **Nekritinė klaida** | Nustatyta klaida ir (ar) problema, kuri kliudo vykdyti būtinas funkcijas, tačiau yra žinomas alternatyvus funkcijos vykdymas arba kai nustatyta klaida, kuri sukelia sunkumus naudojantis sistema, bet neturi įtakos Sistemos funkcijų veikimui ir nedaro jokio kito poveikio Sistemai. |
| **Licencijos** | Paslaugų Teikėjo teikiamos programinės įrangos licencijos, reikalingos Sistemai veikti. |
| **Paslaugos** | Techninio palaikymo, garantijos, diegimo ir duomenų įkėlimo iš esamų sistemų į naują Sistemą, Sistemos pritaikymas Užsakovo poreikiams konfigūruojant, diegiant, Sistemos papildomo vystymo, mokymų paslaugos. |
| **Paslaugų teikimo reglamentas** | Užsakovo su Tiekėju suderintas Sistemos įdiegimo, garantinės aptarnavimo, techninio palaikymo ir vystymo paslaugų teikimo reglamentas, kuriame bus aprašyta, kaip šalys dirba, atsižvelgiant į šioje Techninėje specifikacijoje keliamus reikalavimus. |
| **Prekės** | Sistemos programinė įranga su jai funkcionuoti reikalingomis licencijomis. |
| **Sistema** | Grid Pass |
| **Sutartis** | Sutartis, sudaroma tarp Tiekėjo ir Užsakovo dėl Pirkimo objekto. |
| **Techninė specifikacija** | Šis dokumentas su priedais, kuris laikomas pagrindiniu Pirkimo sąlygų dokumentu, kuriame nurodyti reikalavimai Pirkimo objektui. |
| **Tiekėjas** | Ūkio subjektas – fizinis asmuo, privatusis juridinis asmuo, viešasis juridinis asmuo, kitos organizacijos ir jų padaliniai ar tokių asmenų grupė, su kuriuo Užsakovas sudaro Sutartį. |
| **Užklausa** | Užsakovo prašymas atlikti administravimo, vystymo darbus, nesusijusius su incidento šalinimu. |
| **Užsakymas** | Užsakovo užsakymas tam tikroms Sutartyje numatytoms Prekėms / Paslaugoms. |
| **Užsakovas** | AB „Amber Grid“. |
| **Užsakovo darbo valandos** | Darbo valandos, skaičiuojamos Užsakovo darbo metu: I – IV 7:30 – 16:30 val., V 7:30 – 15:15 val. Darbo dienos trukmė prieš šventines dienas – viena valanda trumpiau. |

1. **PIRKIMO OBJEKTAS, KIEKIAI (APIMTYS) IR PIRKIMO OBJEKTO APRAŠYMAS**
   1. **Pirkimo objektas**

Pagal šią techninę specifikaciją AB „Amber Grid“ siekia įsigyti Grid Pass sistemą (toliau – Sistemą) įskaitant:

1. Sistemos licencijas;
2. Sistemos diegimo ir konfigūravimo paslaugas;
3. Reikalingas integracijas;
4. Sistemos garantinio palaikymo paslaugas;
5. Sistemos techninio palaikymo paslaugas;
6. Sistemos vystymo paslaugas (tobulinimas, vystymas, papildomų duomenų migravimas pagal poreikį, preliminarus kiekis valandomis iki 1000 val.);
7. Mokymus naudotojams (iki 20 val.)

Pasiūlymas turi būti pateiktas visai pirkimų sąlygų techninėje specifikacijos (jos prieduose) nurodytai apimčiai.

* 1. **Esamos situacijos aprašymas**

Esama problema:

* Vadovaujantis Lietuvos Respublikos teisės aktais darbus gamtinių dujų perdavimo sistemos objektuose bei jų įrenginiuose galima atlikti tik gavus perdavimo sistemos operatoriaus (AB „Amber Grid“) raštišką sutikimą tokiems darbams, o saugumui užtikrinti – kaskart atliekant darbus klientai turi registruotis. Kliento prašymai sutikimui gauti pildomi Interneto svetainėje, o leidimai darbams registruojami atskirame Microsoft Forms pagrindu sukurtame klausimyne arba gaunami siunčiami el. paštu. Komunikacija su klientu el. paštu ir / ar telefonu, klientas nemato prašymų būsenų ir neturi galimybės savarankiškai atnaujinti duomenis, jei to riekia sutikimui arba leidimui gauti.
* Sutikimo išdavimo procesas, kuriame apie 95 % viso proceso darbų vyksta rankiniu būdu: rankinis duomenų tvarkymas (nuo kliento prašymo duomenų perkėlimo į sutikimo formą iki sutikimo įkėlimo pasirašymui el. parašu ir siuntimo klientui).
* Klientai apie darbų pradžią praneša skambinant telefonu, darbų pradžios ir pabaigos datos ir laikas ranka įvedami klientų registravimas į el. registrą (Excel).
* Nėra vizualinio kliento darbų atvaizdavimo žemėlapyje, sunku analizuoti gaunamų duomenų kiekį, daug reikšmingos informacijos nugula į darbuotojų el. paštus ir nėra nepasiekiama kitiems darbuotojams.

Siekiama situacija:

* Automatizuotas duomenų registravimas, generavimas.
* Aiškus visiems vienodas veiksmų algoritmas, užtikrinantis greitą užklausų apdorojimą ir efektyvią komunikaciją tarp padalinių ir / ar kliento.
* Ženklus klaidų sumažėjimas.
* Pilnai atsekami visi duomenys ir žingsniai visuose sutikimų bei leidimų procesų etapuose, aktuali informacija.
* Užtikrinti duomenų saugojimo reikalavimai ir terminai pagal BDAR.
* Galimybė generuoti duomenų ataskaitas ir atlikti analizę proceso tobulinti.
* Kliento patirties gerinimas.

**Pagrindinis projekto tikslas** – įsigyti ir įdiegti naują Grid Pass sistemą, kuri pilnai atitiktų teisės aktų reikalavimus, verslo poreikius, būtų patogi ir draugiška naudotojui, nereikalaujant didelių vystymo sąnaudų (t. y. kuo daugiau išpildytų reikalavimus / poreikius baziniais / standartiniais funkcionalumais ar konfigūravimo būdu, be programavimo).

* 1. **Pirkimo objekto aprašymas**
     1. Sistemos ir su ja susijusio Kliento portalo kūrimo, diegimo bei Sistemos, įskaitant Kliento portalą, priežiūros ir vystymo paslaugos.
     2. Preliminarus planuojamų įsigyti Sistemos vystymo paslaugų kiekis yra 1000 val. per 60 (šešiasdešimt) kalendorinių mėnesių nuo Sutarties įsigaliojimo dienos. Sistemos priežiūros ir palaikymo paslaugos įsigyjamos visam Sutarties galiojimo laikotarpiui, už kurias bus mokama kiekvieną kalendorinį mėnesį.
     3. Sistemos diegimo paslaugos turi būti suteiktos planavimo metu suderintais darbų etapais, bet ne vėliau kaip iki 2025 m. gruodžio 31 d.
     4. Sistemos diegimas turi apimti:
        1. Projekto plano parengimą;
        2. Analizę ir projektavimą pagal Užsakovo reikalavimus;
        3. Sistemos licencijų pateikimą;
        4. Sistemos instaliavimą ir konfigūravimą;
        5. Sistemos testavimą ir klaidų taisymą;
        6. Mokymus ir instrukcijų parengimus;
        7. Sistemos bandomąją eksploataciją.
     5. Funkciniai reikalavimai nurodomi: Priedas Nr. 1 Grid\_Pass\_IS\_funkciniai\_reikalavimai.
     6. Nefunkciniai reikalavimai nurodomi šio dokumento TS Nefunkciniai reikalavimai Nr. 5.
     7. Turi būti suprojektuotos ir įdiegtos Sistemos integracijos su kitomis sistemomis, nurodytomis funkciniuose / nefunkciniuose reikalavimuose.
     8. Sistema turi atitikti šių teisės aktų **aktualių redakcijų** reikalavimus :
* 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas, BDAR);
* 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB, (toliau – eIDAS reglamentas)(aktuali redakcija);
* Lietuvos Respublikos kibernetinės saugos įstatymo (aktuali redakcija);
* Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (aktuali redakcija);
* ISO 27001:2022 informacijos saugumo valdymo standarto;
* Jei Sistemos sutarties palaikymo metu priimami nauji arba keičiami galioję LR teisės aktai, Tiekėjas pasikeitimus privalo pritaikyti Sistemoje iki datos, kuri numatyta kaip pokyčių įsigaliojimo diena teisės akte, sutarties sistemos palaikymo paslaugos rėmuose.
  + 1. Reikalavimai paslaugų etapams, terminams ir veikloms
       1. Tiekėjas, remdamasis savo patirtimi ir gerąja praktika per 15 (penkiolika) d. d. turi pasiūlyti ir suderinti su Užsakovu detalų projekto įgyvendinimo planą ir eigą. Projekto įgyvendinimą siūloma vykdyti etapais, nurodytais 2.3.9.2 punkte.
       2. Paslaugų etapai ir veiklos

Žemiau esančioje lentelėje pateikiami pagrindiniai etapai ir numatomi vykdymo terminai.

Terminai:

|  |  |  |
| --- | --- | --- |
| **Projekto įgyvendinimo etapai** | | **Terminas** |
|  | Projekto planavimas | 15 d.d. |
|  | Diegimas | Iki 2025 m. gruodžio 31 d. |
|  | Bandomoji eksploatacija | 2 mėn. |
|  | Garantinis aptarnavimas | 6 mėn. |
|  | Papildomos vystymo paslaugos | Iki sutarties pabaigos |
|  | Techninio palaikymo paslaugos | Iki sutarties pabaigos |

* + - 1. Projekto įgyvendinimo veiklos ir rezultatai:

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | **Etapas** | **Etapo darbai ir veiklos** | **Rezultatas (rengia Tiekėjas)** |
|  | Projekto planavimas | Veiklos metu parengiamas paslaugų teikimo reglamentas, kuriame turi būti apibrėžta (neapsiribojant):   * Projekto tikslai ir uždaviniai; * Projekto planas-grafikas, veiklų ir jų tarpusavio priklausomybių ir atsakomybių, rezultatų ir veiklų įgyvendinimo trukmių aprašas; * Komunikavimo ir rezultatų derinimo procedūra, projekto dalyvių kontaktiniai duomenys; * Rizikos valdymo procedūra; * Pakeitimų valdymas; * Projekto pažangos stebėsena; * Kita projekto valdymui aktuali informacija.   Turi būti Tiekėjo parengtas ir su Užsakovu suderintas veiklų įgyvendinimo grafikas. | Parengtas ir suderintas paslaugų teikimo reglamentas, projekto planas ir grafikas. |
|  | Analizė ir projektavimas | Veiklos metu Tiekėjas susipažįsta su pateikta projekto dokumentacija, vykdo analizės susitikimus su Užsakovo atstovais ir parengia detalios analizės ataskaitą bei detalų projektavimo dokumentą, kuriuose turi būti apibrėžta (neapsiribojant):   * Veiklos procesų schemos ir aprašymai; * Funkcinių ir nefunkcinių reikalavimų detalizavimas ir realizavimo aprašymas; * Integracijų aprašymas; * Sistemos architektūra; * Saugumo reikalavimai; * Reikalavimai infrastruktūrai. | Parengtas ir suderintas bendro sistemos aprašymo dokumentas.  Parengtas ir suderintas Sistemos analizės dokumentas, kuris turi apimti:   * Sistemos specifikaciją; * Sistemos projektavimą; * Sistemos architektūrą; * Sistemos standartines funkcijas; * Sistemos plėtros funkcijas; * Sistemos veiklos procesų aprašą. |
|  | Konfigūravimas / kūrimas | Veiklos metu Tiekėjas turi paruošti techninę dokumentaciją, aprašančią techninę architektūrą, atliktus parametrizavimo, kūrimo darbus. Parengta dokumentacija turi leisti sistemos administratoriams atlikti periodinius darbus, rasti ir šalinti klaidas. Techninė dokumentacija turi apimti (neapsiribojant):   * Techninę architektūrą; * Techninius duomenų srautų aprašymus; * Parametrizavimo aprašymą; * Integracijų aprašymą.   Veiklos metu parengiamos naudotojų ir administratorių instrukcijos.  Veiklos metu Tiekėja parengia naudotojų ir administratorių mokymų planą ir medžiagą.  Veiklos metu parengiamas testavimo planas, metodika bei testavimo scenarijai.  Veiklos metu Tiekėjas organizuoja ir vykdo naudotojų ir administratorių mokymus. | Suprogramuota bei sukonfigūruota Sistema.  Parengta ir suderinta Sistemos techninė dokumentacija.  Parengtos ir suderintos naudotojų ir administratorių instrukcijos.  Parengtas ir suderintas mokymų planas ir mokymų medžiaga.  Parengta ir suderinta vidinių testavimų ataskaita.  Parengtas ir suderintas testavimo planas ir metodika.  Parengti ir suderinti priėmimo testavimo scenarijai. |
|  | Testavimas | Veiklos metu paruošia testavimo duomenis, atlieka konfigūracinius nustatymus, užtikrina kitas technines sąlygas testavimams atlikti.  Tiekėjas pagal testavimo planą ir metodiką turės dalyvauti testavime, teikti konsultacijas kaip turi būti atliekamas testavimas pagal suderintus testavimo scenarijus, informuoti testavimo dalyvius apie klaidos šalinimo terminą, taisyti klaidas. Visa informacija apie klaidų kritiškumo lygį, jos šalinimo terminus, šalinimo eigą ir priskirtus atsakingus asmenis turi būti registruojama klaidų registre. | Atliktas Priėmimo testavimas, kurio rezultatai tenkina testavimo plane numatytus reikalavimus. Parengtos ir suderintos priėmimo testavimo ataskaitos. |
|  | Diegimas | Veiklos metu Tiekėjas turi pasirengti įdiegti gamybinės aplinkos komponentus ir naudotojų aplinkas, sukonfigūruoti integracines sąsajas. Tiekėjas pateikia gamybinės aplinkos instaliacinį paketą kartu su programiniu kodu ir diegimo instrukcija. Tiekėjas atlieka konfigūracinius nustatymus, teikia pagalbą bei konsultacijas būtinų techninių sąlygų užtikrinimui. | Parengtas ir suderintas gamybinės aplinkos instaliacinis paketas ir diegimo instrukcija.  Parengtas ir suderintas bandomosios eksploatacijos planas. |
|  | Bandomoji eksploatacija | Tiekėjas bandomosios eksploatacijos metu pagal suderintą klaidų šalinimo grafiką turi šalinti visus trūkumus, užfiksuotus bandomosios eksploatacijos problemų registre. Tiekėjas turi parengti ir su Užsakovu suderinti garantinio aptarnavimo bei naudotojų konsultavimo reglamentą. | Parengta ir suderinta bandomosios eksploatacijos ataskaita.  Parengtas ir suderintas garantinio aptarnavimo bei naudotojų konsultavimo reglamentas. |
|  | Garantinis aptarnavimas | Turi būti vykdomas garantinis aptarnavimas. | Parengta ir suderinta garantinio aptarnavimo darbų ataskaita. |
|  | Papildomos vystymo paslaugos | Turi būti vykdomi pagal poreikį atsiradę vystymo darbai | Parengtas ir suderintas kiekvieno Užsakymo darbo perdavimo-priėmimo aktas. |
|  | Techninio palaikymo paslaugos | Turi būti vykdoma Sistemos veikimo priežiūra | Parengta ir suderinta kiekvieno mėnesio techninio palaikymo ir atliktų darbų ataskaita bei darbo perdavimo-priėmimo aktas. |

* + - 1. Projekto darbai gali būti vykdomi iteraciniu principu, t. y. visus funkcionalumus padalinus į dalis – iteracijas. Kiekvienas iteracijos apimtyje turi būti vykdomi Analizės ir projektavimo, Konfigūravimo, Testavimo ir Bandomosios eksploatacijos etapai, t. y. informacinės sistemos realizavimas turi vykti prieaugiais (iteracijomis), kurie sudaromi taip, kad per suderintą laiką būtų galima sistemą testuojantiems asmenims pateikti tinkamas testuoti funkcijas arba pagal sukomponuotas User stories sėkmės sąlygas, veikiančias Sistemos testavimo ir gamybinėje aplinkose. Prieaugių (iteracijų) skaičius ir trukmė turi būti optimalūs ir realiai įgyvendinami. Šiuo darbų vykdymo principu siekiama Projekto vykdymą išskaidyti į sudėtines dalis ir viso Projekto metu matyti kuriamus rezultatus (nesukoncentruoti visų diegimo ir testavimo darbų Projekto pabaigai).
      2. Projekto etapų, užduočių ir rezultatų išdėstymo struktūra yra rekomendacinio pobūdžio, todėl Tiekėjas gali siūlyti savo darbų organizavimo planą, paremtą savo Projekto etapų, užduočių ir rezultatų išdėstymo struktūra bei numatytais papildomais rezultatais, kurie Tiekėjo nuomone sukurtų pridėtinę vertę ir nėra nurodyti šiame skyriuje bei bus sukurti Projekto vykdymo metu.
      3. Tiekėjas turi būti oficialus siūlomos Sistemos programinės įrangos gamintojas arba turėti rašytinį susitarimą su gamintoju dėl prekybos siūloma programine įranga, jos diegimo ir techninio palaikymo. Tiekėjas kartu su pasiūlymu turi pateikti dokumentą, patvirtinantį, kad jis yra oficialus siūlomos turinio valdymo programinės įrangos gamintojas arba rašytinį susitarimą su gamintoju dėl prekybos siūloma programine įranga, jos diegimo ir techninio palaikymo.
      4. Tiekėjas privalo Užsakovo vardu užregistruoti licencijų atnaujinimus gamintojo nustatyta tvarka, o registracijos duomenis perduoti Užsakovui.
      5. Tiekėjas įsipareigoja supažindinti Užsakovo atstovus su aktualia gamintojo licencijų sutartimi, taip pat nedelsiant informuoti Užsakovo atstovus atsiradus naujovėms ar pakeitimams gamintojo licencijų sutartyje (taisyklėse).

1. **Sutartinių įsipareigojimų vykdymo tvarka ir terminai**
   1. Ne ilgiau nei per 7 kalendorines dienas nuo sutarties įsigaliojimo dienos turi būti suorganizuotas Tiekėjo susitikimas su AB „Amber Grid“ atstovais. Susitikimo tikslas – susipažinti ir aptarti bendro darbo organizavimą, dokumentus ir jų formą, susiderinti lūkesčius bei aptarti kitus reikiamus klausimus.
   2. Projekto tikslams pasiekti bus sukurta projekto komanda, kurią sudarys AB „Amber Grid“ ir Tiekėjo atstovai.
   3. Projekto metu vykdomi susitikimai ir dokumentacija turi būti rengiami lietuvių kalba. Dokumentacija, kurioje nėra aprašomi veiklos procesai ir funkcijos (diegimo ar administravimo instrukcijos ir pan.), gali būti rengiama anglų kalba prieš tai suderinus su Užsakovu.
   4. Diegimą, konfigūravimą, priežiūros ir vystymo paslaugas teikiantys Tiekėjo specialistai privalo mokėti lietuvių kalbą. Tuo atveju, jei bet kuris čia nurodytus darbus atliekantis specialistas nemoka lietuvių kalbos, Tiekėjas tokiems specialistams privalo užtikrinti vertimą į lietuvių kalbą žodžiu ir raštu be papildomo mokesčio.
   5. Tiekėjas privalo užtikrinti, kad kiekvienas jo siūlomas ir paslaugų teikimui skiriamas komandos narys turėtų reikalingą kompetenciją, žinias arba gebėjimus laiku ir tinkamai įsisavinti informaciją.
   6. Tiekėjas privalo nedelsiant, bet ne vėliau kaip per 14 d. d. informuoti užsakovą, jei keičiasi projekto komandos narys.
   7. Siekiant šioje techninėje specifikacijoje išvardintų rezultatų, Tiekėjas turi užtikrinti efektyvų bendradarbiavimą, paskirti Projektų vadovą, kuris vadovauja Tiekėjo komandai ir:
      1. Teikia projekto eigos ataskaitas (ne rečiau nei 1 k./sav. pagal šalių sutartą formą);
      2. Teikia projektų pakeitimo prašymus, atsiradus nuokrypiams nuo patvirtinto projekto apimties, laiko bei resursų (pagal šalių sutartą formą);
      3. Teikia rezultatų tvirtinimo ataskaitas įvykdžius tarpinį rezultatą pagal nustatytus kriterijus planavimo dokumente (pagal šalių sutartą formą);
      4. Teikia projekto uždarymo ataskaitą su identifikuotomis išmoktomis pamokomis ir galutiniais tvirtinamais rezultatais (pagal šalių sutartą formą);
      5. Dalyvauja susitikimuose:
         1. Ne rečiau nei 2 kartus per mėnesį Projekto komandos susitikime, kuriame pristatoma projekto eiga, sprendžiamos problemos, formuluojamos eskalacijos, įtraukia kitus Tiekėjo komandos narius pagal poreikį.
         2. Ne rečiau nei 1 kartą per mėnesį Projekto valdymo komiteto susitikime, kuriame pristato:
            1. Projekto eigą;
            2. Projekto planą;
            3. Projekto biudžetą;
            4. Projekto problemas ir rizikas;
            5. Pakeitimų prašymus;
            6. Rezultatų tvirtinimo ataskaitas;
            7. Reikalingus sprendimus.
            8. Į komandos ir suinteresuotų šalių susitikimus, įtraukia kitus Tiekėjo komandos narius pagal poreikį.
      6. AB „Amber Grid“ atstovams paprašius, Tiekėjas turės pateikti tarpinius rezultatus, pagal suderintą detalų diegimo darbų grafiką.
      7. Siekiant šioje techninėje specifikacijoje išvardintų rezultatų, Tiekėjas turės užtikrinti apimties, laiko bei resursų valdymą.
      8. Visa projekto metu sukurta arba perduota dokumentacija (planavimo dokumentai, projekto eigos ataskaita, projekto pakeitimo prašymai, rezultatų įgyvendinimą pagrindžiantys dokumentai, priėmimo perdavimo aktai, susitarimai, projekto uždarymo ataskaita, susitikimų protokolai ir kita) turi būti pateikta elektroninėse formose su galimybe redaguoti (pptx, .docx, .xlsx ir kiti formatai). Visos teisės į tokius dokumentus (įskaitant ir intelektinės nuosavybės teisės) priklausys Užsakovui ir bus saugojamos pagal įmonėje galiojančią dokumentų saugojimo tvarką.
      9. Siūlomos Sistemos sprendimas turi suteikti Užsakovui ir trečiosioms šalims teisę be apribojimų keisti, naudoti ir papildyti paslaugos teikimo metu sukurtą / modifikuotą programinį kodą.
      10. Tiekėjas po bandomosios eksploatacijos turi perduoti Užsakovui paslaugos teikimo metu sukurto / modifikuoto programinio kodo išeities kodą, atitinkantį gerąsias programinio kodo formatavimo, kintamųjų bei funkcijų įvardijimo praktikas, ir / arba neužkoduotus sukurto / modifikuoto programinio kodo instaliacinius paketus.
      11. Visi Užsakovo užsakyti ir Tiekėjo suprogramuoti sprendiniai po sutartinių įsipareigojimų pabaigos pereina Užsakovo nuosavybėn kaip ir programinis kodas, atvirame formate. Užsakovas ir trečiosios šalys privalo turėti teisę be apribojimų keisti, naudoti ir papildyti paslaugos teikimo metu sukurtą / modifikuotą programinį kodą.
      12. Klaidos ir vystymo darbai registruojami Tiekėjo IT paslaugų valdymo (toliau ITSM).
2. **Reikalavimai paslaugų teikimui**
   1. **Reikalavimai testavimui:**
      1. Sistemos testavimas atliekamas pagal Tiekėjo parengtą ir su Užsakovu suderintą testavimo planą. Testavimo plane turi būti aprašyti testavimo tikslai, testavimo procesas, atliekami testavimo lygiai, įskaitant priėmimo testavimą (angl. user acceptance testing), ir jų vykdymo pradžios ir baigimo kriterijai, vykdomų testų tipai, testavime dalyvaujančios rolės ir jų atsakomybės, testavimo apimtis, testavimo aplinkos, testavimo įrankiai, testavimo metrikos, testavimo užduotys ir jų atlikimo tvarka bei kita testavimo organizavimui ir atlikimui reikalinga informacija.
      2. Sistemos testavimas apima šiuos lygius: komponento (angl. unit) testavimas, komponentų integracijos (angl. unit integration) testavimas, Sistemos testavimas, Sistemos integracijos su kitomis sistemomis testavimas, priėmimo testavimas.
      3. Visais atvejais Sistemos vystytą programinę įrangą Tiekėjas turi perduoti Užsakovui, tik visiškai ją ištestavęs ir įsitikinęs, kad ją įdiegus nebus sutrikdytas Sistemos arba jos dalies funkcijų ar kitų taikomųjų sistemų darbas ir visi įdiegti pakeitimai veiks taip, kaip buvo numatyta Užsakyme ir kituose dokumentuose, nustatančiuose reikalavimus programinei įrangai.
      4. Sistemos testavimas turi apimti greitaveiką, pasiekiamumą ir kitus scenarijus, suderintus projekto metu.
      5. Tiekėjas atlieka greitaveikos testavimą ir Užsakovo infrastruktūroje esančioje testavimo aplinkoje, pagal jo sukurtus ir su Užsakovu suderintus testavimo scenarijus. Tiekėjas pateikia įrankius ar sprendinius ir paruošia duomenis, reikalingus greitaveikos testavimui atlikti. Duomenų kiekis bus suderintas Analizės etapo metu.
      6. Tiekėjas, sėkmingai atlikęs greitaveikos testavimą testavimo aplinkoje, pateikia testavimo ataskaitą Užsakovui patvirtinti.
      7. Sistemos priėmimo testavimas atliekamas Užsakovo infrastruktūroje esančioje testavimo aplinkoje dalyvaujant Tiekėjui.
      8. Užsakovo atstovai atlieka Sistemos priėmimo testavimą pagal Tiekėjo sukurtus ir su Užsakovu suderintus testavimo scenarijus, skirtus patikrinti funkcinius ir nefunkcinius reikalavimus. Priėmimo testavimo metu surastos klaidos ir neatitikimai funkciniams ar nefunkciniams reikalavimams yra registruojami ir valdomi pagal klaidų valdymo procesą.
      9. Priėmimo testavimo tikslai:
         1. Įsitikinti, kad visi funkciniai ir nefunkciniai Techninės specifikacijos, detalios analizės ir projektavimo dokumentų, naudotojo sąsajos prototipų, integracinių sąsajų specifikacijos bei architektūros dokumentų reikalavimai yra įgyvendinti;
         2. Įsitikinti, kad reikalavimų įgyvendinimas atliktas teisingai ir tinkama apimtimi;
         3. Nustatyti ar Sistema yra tinkama bandomajai eksploatacijai;
         4. Identifikuoti Sistemos klaidas ir neatitikimus pateiktiems reikalavimams.
      10. Priėmimo testavimas yra užbaigiamas, kai tenkinami Sistemos testavimo plane įvardinti sistemos priėmimo kriterijai.
      11. Tiekėjas parengia priėmimo testavimo ataskaitą Užsakovui sėkmingai atlikus Sistemos priėmimo testavimą testavimo aplinkoje.
      12. Užsakovui patvirtinus Sistemos priėmimo testavimo ataskaitą, Sistemos programinė įranga yra diegiama į gamybinę aplinką bandomajai eksploatacijai.
      13. Sudiegus sistemą į gamybinę aplinką atliekamas sistemos saugumo patikrinimas (angl. "Pentest"). Identifikavus pažeidžiamumus:
          1. Kritinio ir aukšto lygio pažeidžiamumai turi būti pašalinti prieš prasidedant bandomajai eksploatacijai;
          2. Vidutinio ir žemo lygio pažeidžiamumai turi būti pašalinti iki bandomosios eksploatacijos pabaigos arba kito suderinto termino;
          3. Po pažeidžiamumų pašalinimo atliekamas pakartotinis saugumo testavimas bei pateikiama patikros ataskaita.
      14. Sistemos saugumo patikrinimas (angl. "Pentest") turi apimti:
          1. Patikrinama tarnybinių stočių operacinės sistemos ir jose veikiančios sisteminės programinės įrangos atnaujinimo lygis ir ar jos nėra pažeidžiamos remiantis patikrinimo dieną žinomomis saugumo spragomis;
          2. Patikrinamas tarnybinių stočių ir jose veikiančios sisteminės programinės įrangos konfigūracijos saugumas;
          3. Patikrinamas prisijungimo prie Tarnybinių stočių saugumas, naudojant anoniminį / nesankcionuotą prisijungimą ir / arba turint eilinio naudotojo prisijungimo duomenis;
          4. Patikrinama ar naudotojai negali eskaluoti savo teisų sistemoje, atlikti veiksmus ir / arba gauti duomenis, nesusijusius su jų tiesioginių pareigų vykdymu;
          5. Patikrinamas duomenų bazės (jei naudojama) atnaujinimo lygis ir konfigūracijos saugumas (laisva prieiga, per didelės naudotojų ar programų teisės, galimybė vykdyti sistemines komandas iš duomenų bazės);
          6. Atlikti WEB aplikacijų taikomųjų programų ir paslaugų saugumo patikrinimą neturint naudotojo prisijungimo ir turint prisijungimus;
          7. Pažeidžiamumų paieška (naudotojo autentifikavimo mechanizmo patikrinimas, sesijos vientisumo patikrinimas, įvedamos informacijos apdorojimo patikrinimas, programinio kodo integralumo patikrinimas, klaidų pranešimų apdorojimas, sisteminės informacijos atskleidimas, serviso konfigūravimo klaidos) automatizuotais WEB pažeidžiamumo skeneriais;
          8. Sistemos saugumo spragų patikrinimas pagal OWASP Top 10, REST/SOAP/GraphQL API Testing ir kiti.
      15. Sistemos saugumo patikrinimo paslaugai atlikti pasitelkiama trečioji šalis, suderinant šios paslaugos užsakymą su Užsakovu.
   2. **Reikalavimai bandomajai eksploatacijai**
      1. Bandomoji eksploatacija yra atliekama Sistemos gamybinėje aplinkoje įdiegus Sistemos funkcionalumo paketus.
      2. Bandomosios eksploatacijos trukmė ne daugiau kaip 2 mėnesiai nuo paskutinio Sistemos funkcionalumo paketo įdiegimo. Jei projektas bus vykdomas iteraciniu principu, tai visų iteracijų bandomoji eksploatacija turi baigtis kaip ir paskutinio Sistemos funkcionalumo paketo įdiegimo bandomoji eksploatacija.
      3. Tiekėjas turi parengti ir suderinti su Užsakovu bandomosios eksploatacijos planus, kurių tikslas – aprašyti bandomosios eksploatacijos metodiką (pasiruošimo eiga, klaidų stebėjimas, bandomosios eksploatacijos pabaigos kriterijai), įvedimo į bandomąją eksploataciją veiklų grafiką.
      4. Bandomosios eksploatacijos tikslas – patikrinti Sistemos veikimą gamybinėje aplinkoje, išbandyti gamybinę sistemos komponentų konfigūraciją, identifikuoti ir pašalinti bandomosios eksploatacijos metu pastebėtus defektus, stabilizuoti gamybinės aplinkos konfigūraciją, atsižvelgiant į bandomosios eksploatacijos metu sukauptą patirtį, įsitikinti duomenų vientisumu ir teisingumu, įsitikinti Sistemos integracijų su išorinėmis ar vidinėmis sistemomis teisingu ir saugiu veikimu.
      5. Sistemos veikimas turi būti užtikrintas visos bandomosios eksploatacijos metu.
      6. Bandomosios eksploatacijos metu Tiekėjas turi teikti intensyvias sistemos aptarnavimo ir naudotojų konsultavimo paslaugas.
      7. Esant poreikiui ir Užsakovui paprašius, Tiekėjas turi suteikti konsultacijas dėl Sistemos veikimo vietoje, t. y. Paslaugų teikimo vietoje (Užsakovo patalpose).
      8. Bandomosios eksploatacijos metu turi būti taisomos identifikuotos klaidos.
      9. Tiekėjas bandomosios eksploatacijos metu turi šalinti visus identifikuotus defektus bei pastebėtus neatitikimus.
      10. Defektų šalinimas vykdomas standartine tvarka: taisomas programos kodas (jei būtina), ruošiamas Sistemos pokyčio dokumentas, pokytis testuojamas Sistemos testavimo aplinkoje ir tik po to pokyčio diegimas atliekamas Sistemos gamybinėje aplinkoje.
      11. Į bandomosios eksploatacijos trukmę neįskaičiuojamas laikas, kai dėl Sistemos esminių klaidų tokia bandomoji eksploatacija negalėjo vykti.
      12. Bandomoji eksploatacija yra baigiama, kai tenkinami bandomosios eksploatacijos priėmimo kriterijai, kurie pateikiami bandomosios eksploatacijos plane.
      13. Tiekėjas bandomosios eksploatacijos pabaigoje turi pateikti bandomosios eksploatacijos ataskaitą.
      14. Dokumente turi būti pateiktas bandomosios eksploatacijos metu rastų klaidų sąrašas, atliktų veiklų vertinimas, bandomosios eksploatacijos rezultatų atitikimas priėmimo kriterijams, ir siūloma išvada dėl bandomosios eksploatacijos pabaigos.
      15. Sėkmingai baigus etapo bandomąją eksploataciją yra pasirašomas atitinkamo Sistemos etapo perdavimo aktas.
      16. Tik pasirašius visos sistemos perdavimo aktą po bandomosios eksploatacijos bus laikomas sistemos diegimo projekto užbaigimu, ir bus pradėtas skaičiuoti garantinio aptarnavimo terminas.
   3. **Reikalavimai garantiniam aptarnavimui**
      1. Sistemos garantinis aptarnavimas, t. y. priežiūros be papildomo užmokesčio, sąlygos turi tenkinti žemiau pateiktus reikalavimus.
      2. Garantinio aptarnavimo objektas yra pagal šios techninės specifikacijos reikalavimus įdiegta Sistema su visomis jai priklausančiomis sąsajomis, licencijomis ir dokumentacija.
      3. Paslaugų teikėjas ne mažiau kaip 6 mėnesių po visos Sistemos bandomosios eksploatacijos etapo užbaigimo ir galutinio darbų perdavimo ir priėmimo aktų pasirašymo dienos turi atlikti garantinį aptarnavimą.
      4. Sistema privalo būti darbinga, patikima, nustatytais terminais atstatoma po klaidų. Visi Paslaugų teikėjo veiksmai atliekant garantinį aptarnavimą turi būti atliekami pagal su Užsakovu suderintą tvarką.
      5. Garantinis aptarnavimas apima:
         1. Dalyvavimą Sistemos ir su Sistema susijusių klaidų sprendime;
         2. Sistemos neatitikimų funkciniams bei nefunkciniams reikalavimams ir veikimo klaidų šalinimą bei kitas LR įstatymais ir norminiais aktais numatytas kokybės garantijas;
         3. Eksploatuojamos Sistemos darbingumo atstatymą, pvz., įvykus duomenų bazės ar atskirų jos komponentų darbų sutrikimams, kai tai įvyksta dėl Tiekėjo pateiktų pakeitimų atnaujinimų ar kitų Tiekėjo veiksmų ar neveikimo. Tiekėjo neveikimu yra laikomas Tiekėjo nesiėmimas jokių veiksmų, kai sistemos eksploatacijos metu yra aptinkamas duomenų bazių ar atskirų jos komponentų darbų sutrikimas, arba, Tiekėjui neinformuojant Užsakovo apie gamintojo jam pateiktus sistemos atnaujinimus (kurie turi ar gali turėti įtakos tinkamam sistemos funkcionavimui).
         4. Sugadintų duomenų atkūrimą, kai gedimo priežastis yra Tiekėjo pateiktos programinės įrangos netinkamas veikimas;
         5. Konsultacijų telefonu ir elektroniniu paštu darbo dienomis Lietuvos laiku (detalus laikas bus suderintas rengiant ir derinant paslaugų vykdymo reglamentą) teikimą Sistemos naudotojams sistemos naudojimo, fiksuotų problemų ir veikimo nedokumentuotais klausimais. Numatomas naudotojų skaičius iki 6.
         6. Neatitikimų šalinimą ir sistemos sutrikimų taisymą, kai Tiekėjo siūlomas sprendimas neveikia ar funkcionuoja neteisingai ne dėl to, kad netinkamai realizuotas funkcinis / nefunkcinis reikalavimas ar veikimo logika, o dėl kitų Tiekėjo pateiktų sudėtinių sprendimo dalių. Tokių neatitikimų pavyzdžiai: pateiktas standartinis sistemos funkcionalumas daro netinkamą įtaką (nepilnai ar neteisingai saugomi duomenys) funkcinių reikalavimų rezultatams, pateikta duomenų bazių valdymo sistema daro netinkamą įtaką funkcinių reikalavimų rezultatams (pvz.: sistemos greitaveikai).
      6. Teikiant Sistemos garantinio palaikymo paslaugas visi kreipiniai turi būti registruojami Tiekėjo ITSM.
      7. Detalios garantinio aptarnavimo teikimo procedūros ir darbo tvarkos bus derinamos rengiant garantinio aptarnavimo bei naudotojų konsultavimo reglamentą.
      8. Tiekėjas parengs garantinio aptarnavimo bei naudotojų konsultavimo reglamentą.
      9. Informacija apie pašalintas (pataisytas) Klaidas ataskaitos forma turi būti atnaujinama ir pateikiama kartą per mėnesį.
      10. Sistemos funkcionalumo atnaujinimui, atlikus darbus, suteikiamas ne trumpesnis nei 6 mėnesių garantinio aptarnavimo laikotarpis, skaičiuojant nuo Sistemos funkcionalumo atnaujinimo versijos pateikimo Užsakovui ir Užsakovo tinkamo veikimo patvirtinimo momento.
   4. **Reikalavimai techninio palaikymo paslaugoms**
      1. Sistemos techninio palaikymo paslaugos teikiamos pagal mėnesinį mokestį po visos Sistemos bandomosios eksploatacijos etapo užbaigimo ir galutinio darbų perdavimo ir priėmimo aktų pasirašymo dienos iki sutarties galiojimo pabaigos.
      2. Užsakovas neįsipareigoja užsakyti ir nupirkti visų techninėje specifikacijoje numatytų techninio palaikymo paslaugų.
      3. Visi Tiekėjo veiksmai, susiję su techninio palaikymo paslauga turi būti vykdomi pagal suderintas su Užsakovu procedūras.
      4. Šalių susitarimu, Sistemos techninio palaikymo paslaugos gali būti teikiamos Užsakovo ne darbo metu.
      5. Sistemos techninio palaikymo paslaugos neįeina į garantinio aptarnavimo ir vystymo paslaugas (žr. skyrius *4.3 Reikalavimai garantiniam aptarnavimui* ir *4.5* *Reikalavimai vystymo paslaugoms*).
      6. Sistemos techninio palaikymo paslaugos apima:
         1. Sistemos incidentų, klaidų dėl kurių Užsakovas kreipiasi į Tiekėją, kai sistemos darbo problemų neišsprendžia Užsakovo administravimo specialistai, sprendimas. Sistemos darbo problemų, kurios kilo dėl vystymo paslaugų jų garantiniu laikotarpiu, sprendimas neįeina į sistemos techninio palaikymo paslaugų imtį;
         2. Sistemos incidentų sprendimą;
         3. Sistemos taisymus pastebėtų klaidų ar duomenų vientisumo pažeidimo atvejais;
         4. Sistemos kodo pokyčius, susijusius su Sistemos veikimo problemomis po atliktų Sistemoje naudojamos kitos programų įrangos naujinimų (angl. „patches“, „updates“, „upgrades“);
         5. Sistemos dokumentų ruošimą ir pateikimą;
         6. Sistemos dokumentacijos reguliarų naujinimą;
         7. Konsultavimą Sistemos naudojimo, fiksuotų problemų ir veikimo klausimais;
         8. Programinės įrangos sutrikimų šalinimas – skubi pagalba, sutrikus sistemos ar ją sudarančių komponentų veikimui, net jei sistemos sutrikimas atsirado ne dėl Tiekėjo kaltės – problemų diagnostika ir sistemos funkcionavimo atstatymas;
         9. Programinės įrangos pataisymų, klaidų šalinimo diegimus;
         10. Sistemos versijos atnaujinimus, kurie turi būti atliekami suderinus atnaujinimą su Užsakovu.
      7. Teikiant Sistemos techninio palaikymo paslaugas visi kreipiniai turi būti registruojami Paslaugų teikėjo ITSM.
      8. Paslaugų vykdymo metu modifikuotas, atnaujintas ar pakeistas Sistemos funkcionalumas Užsakovui turi būti perduotas tik Tiekėjui pilnai jį ištestavus Tiekėjo kūrimo aplinkoje. Tiekėjas perduoda Užsakovui diegimą į testavimo aplinką, kurioje testuojama ir tik įsitikinus, kad visi įdiegti pakeitimai veiks taip, kaip buvo numatyta, bei gavus Užsakovo patvirtinimą – diegiami darbinėje aplinkoje. Tiekėjo pateiktus diegimo paketus testavimo ir darbinėje aplinkose vykdo Užsakovas. Tiekėjui ir Užsakovui sutarus kitaip, diegimo į aplinkas tvarka gali būti pakeista.
      9. Tiekėjas kiekvieną kalendorinį mėnesį teikia techninio palaikymo paslaugų ataskaitą apie suteiktas techninio palaikymo paslaugas, detalizuoja atliktas paslaugas, aprašo išspręstas problemas. Ataskaita pateikiama vieną kartą per mėnesį, ne vėliau kaip per 5 darbo dienas po mėnesio, per kurį buvo suteiktos techninio palaikymo paslaugos, pabaigos.
      10. Techninio palaikymo paslaugos turės būti teikiamos visam Sistemos funkcionalumui, tiek standartiniam, tiek sukurtam, pritaikant pagal Užsakovo poreikius.
   5. **Reikalavimai vystymo paslaugoms**
      1. Sistemos vystymo paslaugos neįeina į garantinio aptarnavimo paslaugas (žr. skyrių *4.3 Reikalavimai garantiniam aptarnavimui*).
      2. Vystymo paslaugos kyla dėl pasikeitusių aplinkybių bei užsakovo poreikių ir apima Sistemos papildomo ir ankstesnėje sistemos versijoje nenumatyto funkcionalumo sukūrimą ar esančio funkcionalumo pakeitimą.
      3. Sistemos vystymo paslaugų užsakymai turi būti registruojami Tiekėjo ITSM.
      4. Tiekėjas per 5 d. d. turi pateikti vystymo paslaugų įvertinimą, atsižvelgiant į Užsakovo pokyčių (vystymo) įgyvendinimo galimybę, suderinamumą ir tinkamumą. Jei dėl objektyvių vienos (ar abiejų) šalių vėlavimo priežasčių yra reikalingas paslaugų įvertinimo termino pratęsimas, terminas gali būti pratęstas tik abiem šalims iš anksto sutarus ir raštu patvirtinus naują paslaugų įvertinimo terminą. Naujas paslaugų įvertinimo terminas derinamas ir tvirtinamas su Užsakovo paskirtu už sutarties vykdymą atsakingu atstovu.
      5. Vystymo paslaugų užsakymas bus laikomas gautu kitą darbo dieną nuo jo registravimo Užsakovo dienos. Tiekėjas vystymo paslaugas pradeda teikti tik gavęs (ITSM ar kita su Užsakovu suderinta forma) užpildytą Sistemos vystymo paslaugų užsakymą.
      6. Kiekvienu atskiru atveju, prieš pradedant teikti vystymo paslaugas, Tiekėjas turės pateikti (detalizuoti) ir su Užsakovu suderinti planuojamų atlikti paslaugų aprašymą, pateikiant laiko sąnaudų pagrindimą bei įgyvendinimo terminą.
      7. Užsakovas, gavęs vystymo paslaugų Užsakymo įgyvendinimui būtinų veiklų aprašymą ir apimčių įvertinimą, priima sprendimą dėl Užsakymo įgyvendinimo:
         1. Jei nusprendžiama, kad vystymo paslaugos, nurodytos Užsakyme, yra nereikalingos dėl netinkamo kaštų ir naudos santykio – Užsakymas yra atšaukiamas apie tai informuojant Tiekėją. Jei įvertinimo aprašymas yra neaiškus, Užsakovas gali paprašyti Tiekėjo detalizuoti Sistemos pakeitimo įvertinime aprašytas paslaugas bei jų teikimo laiko sąnaudų įvertinimą. Tiekėjas privalo atsakyti į Užsakovo pateiktus klausimus;
         2. Jei nusprendžia, kad vystymo paslaugos, nurodytos Užsakyme, yra reikalingos, vystymo paslaugų detali analizė, suteikimo terminai, apimtys ir sąmata yra raštu patvirtinami Užsakyme. Už apimtis (darbo valandų kiekį), kurios nebuvo suderintos (t. y. kurios nebuvo nurodytos Užsakyme) Užsakovas nemoka.
      8. Vystymo paslaugos turi būti atliekamos vadovaujantis sekančiais etapais:
         1. Analizės etapas: Šiame etape Tiekėjas bendrauja su Užsakovu ir išsiaiškina jo tikslus, poreikius ir lūkesčius, susijusius su IT sistema. Tiekėjas taip pat atlieka rinkos ir konkurencijos tyrimus, kad nustatytų galimus IT sistemos sprendimus ir jų privalumus ir trūkumus. Analizės etapo rezultatas yra IT sistemos specifikacija ir reikalavimai, kurie apibrėžia sistemos funkcionalumą, veikimą, saugumą ir kitus kriterijus.
         2. Projektavimo etapas: Šiame etape Tiekėjas pasirenka tinkamą IT sistemos architektūrą ir dizainą, kuris atitiktų IT sistemos reikalavimus ir užtikrintų jos veikimą, suderinamumą, plečiamumą ir saugumą. Projektavimo etapo rezultatas yra IT sistemos komponentų, sąsajų, duomenų modelių, algoritmų ir kitų elementų apibrėžimas ir projektavimas.
         3. Kūrimo etapas: Šiame etape Tiekėjas programuoja ir koduoja IT sistemos komponentus, naudodamas pasirinktas programavimo kalbas, įrankius ir metodologijas. Kūrimo etapo rezultatas yra IT sistemos programinė įranga, kuri realizuoja sistemos funkcionalumą ir atitinka sistemos reikalavimus.
         4. Testavimo etapas: Šiame etape Tiekėjas atlieka nuodugnų ir kokybišką IT sistemos testavimą, kuris patikrina IT sistemos funkcionalumą, veikimą, saugumą ir kitus aspektus. Testavimo etapo rezultatas yra IT sistemos testavimo scenarijai, duomenys, metodai ir įrankiai, taip pat testavimo rezultatų dokumentacija ir analizė, o rastos klaidos ir defektai yra taisomi tiekėjo sąnaudomis ir patikrinami pakartotinai.
         5. Diegimo etapas: Šiame etape Tiekėjas instaliuoja ir konfigūruoja IT sistemą kliento aplinkoje, taip pat atlieka IT sistemos integraciją su kitomis IT sistemomis, su kuriomis ji turi sąveikauti. Diegimo etapo rezultatas yra IT sistemos sėkmingas paleidimas ir pradėjimas naudoti.
         6. Priežiūros etapas: Šiame etape Tiekėjas teikia IT sistemos palaikymo ir priežiūros paslaugas, kurios apima IT sistemos atnaujinimus, pakeitimus, praplėtimus ir kitus vystymo ciklus, taip pat IT sistemos veiklos stebėseną, vertinimą ir optimizavimą. Priežiūros etapo rezultatas yra IT sistemos nuolatinis tobulinimas, atsižvelgiant į technologijų pokyčius, naudotojų poreikius ir rinkos tendencijas.
      9. Sistemos vystymo paslaugų užsakymų skaičius yra neribojamas, tačiau bendras užsakymų vykdymui skirtas darbo valandų skaičius negali viršyti sutartyje numatyto maksimalaus vystymo paslaugoms skirto valandų skaičiaus.
      10. Paslaugų vykdymo metu modifikuotas, atnaujintas ar pakeistas Sistemos funkcionalumas turi būti pilnai jį ištestuotas Tiekėjo kūrybinėje aplinkoje, ir tada gali būti diegiamas Užsakovo testavimo aplinkoje. Tiekėjas, įdiegęs naują funkcionalumą testavimo aplinkoje, pirmiausia perduoda Užsakovui testuoti, ir tik įsitikinus, kad visi įdiegti pakeitimai veiks taip, kaip buvo numatyta, bei gavus Užsakovo patvirtinimą – diegiami darbinėje aplinkoje. Tiekėjui ir Užsakovui sutarus kitaip, diegimo į aplinkas tvarka gali būti pakeista.
      11. Tiekėjas yra atsakingas už Sistemos dokumentacijos atnaujinimą atsižvelgiant į suteiktų vystymo paslaugų įneštus pokyčius tiek Sistemos konfigūracijai, tiek ir funkcionalumui.
      12. Tiekėjas, tinkamai įvykdęs vystymo paslaugų užsakymą, kreipiasi į Užsakovą raštu ir pateikia Užsakovui pasirašyti vystymo paslaugų užsakymo perdavimo – priėmimo aktą, kuris rengiamas kiekvienai Užsakovo pateiktai vystymo paslaugų užsakymo formai.
      13. Esant situacijai, kad suteiktų vystymo paslaugų perdavimo – priėmimo metu Užsakovas negali patikrinti visų suteiktų vystymo paslaugų atitikimo Užsakyme nustatytiems reikalavimams, todėl Šalys susitaria, kad vystymo paslaugų perdavimo – priėmimo akto pasirašymas jokiu būdu neapriboja Užsakovo teisės reikalauti trūkumų ištaisymo ir tuo pačiu įpareigoja Tiekėją ištaisyti klaidas ar neatitikimus pagal Užsakymo vystymui turinį.
      14. Užsakovas neįsipareigoja įsigyti visų numatytų Sistemos funkcionalumo vystymo paslaugų valandų.
      15. Tiekėjas vystymo paslaugoms suteikia kokybės garantiją, kuri galioja visoms suteiktų vystymo paslaugų sudėtinėms dalims 12 mėnesių nuo priėmimo–perdavimo akto už vystymo paslaugas pasirašymo dienos. Jeigu Užsakovas negali naudotis suteiktomis vystymo paslaugomis, kurioms yra nustatytas kokybės garantijos terminas, dėl nuo Tiekėjo priklausančių kliūčių, tai garantijos terminas neskaičiuojamas tol, kol Tiekėjas tas kliūtis pašalina. Garantijos terminas pratęsiamas tokiam laikui, kurį Užsakovas negalėjo suteiktų vystymo paslaugų naudoti dėl trūkumų.
      16. Kokybės garantijos laikotarpiu, Tiekėjas privalo užtikrinti produkto ar komponento saugumą, jei kokybės garantijos laikotarpyje identifikuotas pažeidžiamumas, Tiekėjas privalo tokį pažeidžiamumą pašalinti nemokamai per protingą terminą, kuris yra derinamas su Užsakovu atskirai.
      17. Vystymo paslaugos vykdomos vadovaujantis šios Techninės specifikacijos **Reikalavimai infrastruktūrai ir architektūrai** ir **Sistemos saugos reikalavimai** punktuose.
      18. Sistemoje atliekant pakeitimą ir / ar atnaujinimą, turi būti galimybė užtikrinti, kad:
          1. Visi saugomi duomenys bus perkelti į naują duomenų bazės struktūrą;
          2. Bus išlaikytas duomenų vientisumas ir integralumas;
          3. Jokie saugomi duomenys nebus prarasti;
          4. Nebus sutrikdytas Sistemoje realizuotas funkcionalumas.
      19. Sistemos techninės ir / arba programinės įrangos modifikavimas, tobulinimas ir klaidų taisymas negali turėti įtakos anksčiau įvestų duomenų vientisumui.
      20. Įdiegus naują funkcionalumą, ne vėliau kaip per 5 (penkias) darbo dienas nuo priėmimo perdavimo akto pasirašymo, Tiekėjas Užsakovui, jei funkcionalumo užsakyme nesutarta kitaip, turi pateikti toliau aprašytas dokumentaciją, kuri privaloma sistemos administratoriui ir naudotojui:
          1. Techninė dokumentacija:
             1. Techninė specifikacija: Išsami informacija apie naują funkcionalumą ar modulį, įskaitant techninius aspektus, sąsajas su kitomis sistemomis ir kitas technines detales.
             2. Diegimo instrukcijos: Žingsnis po žingsnio nurodymai, kaip įdiegti naują funkcionalumą ar modulį. Tai gali apimti reikiamus konfigūracijos žingsnius ir priklausomybes nuo kitų komponentų.
          2. Naudotojo dokumentacija:
             1. Naudotojo vadovas: Suprantamas ir lengvai skaitomas dokumentas, skirtas sistemos naudotojui. Jis turėtų apimti informaciją apie naują funkcionalumą, naudojimo instrukcijas ir galbūt pavyzdžius.
             2. Mokomoji medžiaga: Papildoma informacija, tokia kaip mokomieji vaizdo įrašai ar pavyzdžiai, kurie gali padėti naudotojams greičiau suprasti sudiegtas naujoves.
          3. Testavimo dokumentacija:
             1. Testavimo ataskaitos: Aprašymai ir rezultatai iš testavimo, atlikti tiekėjo pusėje. Tai svarbu, kad būtų aišku, kaip buvo tikrinama naujo funkcionalumo veikimas.
          4. Sistemos priežiūros dokumentacija:
             1. Priežiūros vadovas: Informacija apie tai, kaip prižiūrėti ir palaikyti naują funkcionalumą. Įskaitant galimus problemų sprendimo būdus ir poreikį atnaujinti arba keisti parametrus.
3. **Nefunkciniai reikalavimai**
   1. **Reikalavimai Licencijoms**
      1. Sistemos licencijos gali būti nuolatinės (angl. perpetual) arba pateiktos nuomos būdu (angl. subscription).
      2. Sistemos licencijų kaina yra sudėtinė Sistemos įdiegimo paslaugos kainos dalis.
      3. Planuojamas Kliento portalo naudotojų skaičius 400, ir 100-as vidinių sistemos naudotojų. Kartu su pasiūlymu tiekėjas turi pateikti papildomų licencijų, jų palaikymo bei susijusių kaštų įkainius. Užsakovas gali papildomai įsigyti trūkstamų licencijų apmokant už jas pagal sutartyje numatytus įkainius.
      4. Paslaugų Teikėjas turi pasiūlyti tokią licencijų apimtį, kuri tenkina visus Pirkėjo keliamus funkcinius, nefunkcinius ir kitus reikalavimus. Jei Sistemos diegimo eigoje paaiškės, kad tam tikriems reikalavimams įgyvendinti yra reikalinga didesnė licencijų apimtis, Paslaugų Teikėjas turės pateikti visas trūkstamas reikalingas licencijas savo sąskaita. Išskyrus tuos atvejus, kai Pirkėjas išplečia ar pakeičia pirkimo objekto apimtį numatytą Sutartyje.
      5. Licencijos naujinimai ir programinės licencinės įrangos garantinis aptarnavimas turi būti teikiamas įsigytos licencijos apimtyje.
      6. Visoms aplinkoms be papildomo mokesčio, ar kitaip apmokestinant turi būti suteiktos Sistemos licencijos (jeigu tokios reikalingos), tokiu pačiu kiekiu kaip ir gamybinėje aplinkoje.
      7. Jeigu bus naudojamos nuolatinės (angl. perpetual) licencijos, tai pasibaigus Sistemos licencijų palaikymo galiojimo terminui, Sistemos darbas neturi sustoti.
      8. Licencijų gamintojo palaikymo laikotarpis turi galioti visą Sutarties galiojimo terminą.
      9. Tiekėjas Užsakovui turi pateikti visas (Sistemos ir trečiųjų šalių) licencijas, būtinas Sistemai diegti ir veikti visą sutarties laikotarpį.
      10. Pateiktos licencijos privalo būti suderinamos su Microsoft Azure aplinka ir negali būti pririšamos prie konkrečios serverinės dalies (IP adresas, MAC adresas, Procesorius ir t. t.).
      11. Tiekėjas turi užtikrinti, kad Sistemos ir su ja susijusioms paslaugoms būtų naudojama tik legali programinė įranga.
      12. Trečiųjų šalių mokamos programinės įrangos licencijos kaina ir palaikymo (angl. support) kaštai turi galioti visą Sutarties galiojimo laikotarpį bei įtraukti į bendrą pasiūlymo kainą. Tiekėjas privalo įvertinti ir nurodyti visas programinės įrangos licencijavimo sąlygas, įskaitant atvejus, kai programinė įranga yra nemokama tik asmeniniam naudojimui, bet reikalauja licencijos komerciniam (verslo) naudojimui. Tokia programinė įranga turi būti laikoma mokama ir įtraukta į pasiūlymo kaštus, jei jos naudojimas verslo aplinkoje reikalauja licencijos.
   2. **Reikalavimai infrastruktūrai ir architektūrai**
      1. Sistema turi būti įdiegta Užsakovo turimoje infrastruktūroje arba Užsakovo turimoje M365 paslaugoje.
      2. Sistema turi būti realizuota ne mažiau kaip pagal trijų lygių programų architektūros modelį (duomenų bazės lygis, aplikacijų lygis, naudotojo sąsajos lygis). Sistemoje turi būti galimybė konfigūruoti ir plėsti kiekvieną iš šių lygių individualiai, nepriklausomai nuo kitų lygių.
      3. Visi sistemos komponentai turi būti diegiami į virtualius serverius arba turi veikti konteinerių pagrindu, išskyrus atvejus jeigu sistema diegiama užsakovo turimoje M365 paslaugoje.
      4. Sistema turi turėti integraciją su Užsakovo MS Entra ID ir būti pritaikyta saugiai pasiekti iš bet kur ir iš bet kokio įrenginio. Integracijos realizacija Užsakovas rūpinsis pats, o Tiekėjas suteiks reikalingą pagalbą.
      5. Suspendavus naudotoją Užsakovo Microsoft Entra ID paslaugoje, naudotojas turi būti suspenduotas Sistemoje. Periodiškumas turi būti laisvai užsakovo konfigūruojamas.
      6. Įsigyjant programinės įrangos licencijas, turi būti galimybė naudotis virtualizacijos / konteinerių valdymo platformoje, išskyrus atvejus kai diegiama Užsakovo turimoje M365 paslaugoje.
      7. Užsakovas šiuo metu diegia ir plėtoja Atviro kodo duomenų bazes „PostgreSQL bei MySQL“ ir komercinę Microsoft SQL Server „Standard Edition“.
      8. Turi būti numatytos produkcinė ir testavimo aplinkos, atskirtos viena nuo kitos su pilnai realizuotais funkcionalumais. Kūrybinė aplinka (vystymo) turi būti realizuota Tiekėjo aplinkoje (Tiekėjo infrastruktūroje).
      9. Sistemos programinė įranga turi palaikyti Sistemos pajėgumų plėtrą, prijungiant papildomą techninę įrangą, t. y. Sistemos greitaveika turi būti nesunkiai didinama pridedant papildomus techninius išteklius, nekeičiant programinės įrangos išeities tekstų. Techninės įrangos pajėgumų (išskyrus atvejus, kai sistema diegiama M365 paslaugoje) didinimas turi būti atliekamas nestabdant, kiek tai įmanoma, Sistemos darbo.
      10. Sistemos papildomų funkcijų pridėjimas turi būti galimas įdiegiant gamintojo arba paties Teikėjo sukurtus plėtinius.
      11. Sistema turi būti suprojektuota ir realizuota taip, kad būtų lanksti modifikuojant – realizavus funkcionalumo pakeitimus vienoje ar keliose funkcinėse srityse, pakeitimai neturi būti visos Sistemos perkūrimo priežastimi.
      12. Sistemos techninės ir / arba programinės įrangos modifikavimas, tobulinimas ir klaidų taisymas negali turėti įtakos anksčiau įvestų duomenų vientisumui.
      13. Sistemoje neturi būti įkoduotų (angl. Hard Coded) duomenų, kuriems koreguoti ir / ar keisti būtų reikalingos Tiekėjo paslaugos.
      14. Duomenų tvarkymas turi atitikti Lietuvos Respublikos raštvedybos taisykles (skaitmenų formatas, datos ir laiko formatai, kt.).
      15. Sistemoje turi būti vykdomas duomenų formato korektiškumo tikrinimas duomenų laukų lygiu (pvz., asmens varde neturi būti skaičių, kt.) ir duomenų laukų grupių lygiu (pvz., paieškos pradžios data turi būti ankstesnė už paieškos pabaigos datą, kt.). Prieš išsaugant įvestus duomenis, turi būti atliktas išsamus duomenų korektiškumo patikrinimas (pvz., patikrinimas, ar visuose būtinuose duomenų laukuose įvesti duomenys, kt.). Duomenų laukai, kurių korektiškumas turi būti tikrinamas, turės būti suderinti Projekto metu.
      16. Sistema turi užtikrinti importuojamų duomenų integralumą:
          1. Aptikus klaidas importuojamuose duomenyse, nėra importuojami jokie duomenys;
          2. Aptikus klaidas importuojamuose duomenyse, turi būti atskirai pateikti klaidingi duomenys bei įvardintos jų klaidos.
          3. Detalios duomenų importavimo taisyklės turės būti suderintos Projekto metu.
      17. Sistemoje turi būti galimybė suformuoti naudotojų ataskaitą, apimančią naudojimosi informacija (pvz., prisijungimo ir naudojimosi laikai).
      18. Visi sistemos moduliai turi būti glaudžiai integruoti vienas su kitu ir pildant / keičiant duomenis vienoje vietoje, turi būti užtikrintas automatinis atnaujinimas kitose susijusiose vietose.
      19. Sistema turi būti suderinta ir palaikyti hibridines integracijų tarp sistemų sąsajas (angl. On Cloud ir On Site).
      20. Turi būti realizuota Integracija su Microsoft 365 Apps for Enterprise sutikimams ir / arba leidimams peržiūrėti, redaguoti ir tvirtinti.
      21. Sistemos greitaveika turi būti ne mažesnė nei: didžiausios formos atidarymo laikas ne ilgiau nei 2 (dvi) sek., duomenų išsaugojimo operacija po pakeitimo formoje turi trukti ne ilgiau nei, 2 (dvi) sek., kliento veiksmai su procesais turi trukti ne ilgiau nei, 3 (tris) sek. Ilgiau kaip 3 (tris) sekundes trunkantys sistemos procesai, turi būti vizualiai pateikti ekrane, naudojant momentinį pranešimą su progreso indikatoriumi. Sistema turi veikti pagal aukščiau paminėtus greitaveikos parametrus, net tuomet kai su sistema dirba visi naudotojai vienu metu. Tiekėjas Užsakovui turi pateikti Sistemos infrastruktūrai keliamus pagrįstus reikalavimus, siekiant užtikrinti greitaveikos reikalavimų atitikimą.
      22. Visi sisteminiai pranešimai (informaciniai, klaidos ir panašiai) turi būti aiškūs ir suprantami naudotojui, pateikti lietuvių arba anglų kalba, priklausomai nuo naudotojo pasirinktos Sistemos atvaizdavimo kalbos.
      23. Sistemos operacijos duomenų bazėje gali būti atliekamos tik per Sistemos aplikacijos sluoksnį.
      24. Sistemoje turi būti priemonės, užtikrinančios vieningą duomenų suvedimą (angl. Single Data Entry), t. y. suvedus tam tikrą duomenų reikšmę, pvz., objekto pavadinimą, tam pačiam Sistemos objektui dubliuojančių reikšmių suvedimas nebūtų galimas ir pan.
      25. Sistemoje turi būti realizuota galimybė siųsti elektroninius laiškus Sistemos naudotojams.
   3. **Reikalavimai integracinėms sąsajoms**
      1. Integracijos su Užsakovo naudojamomis informacinėmis sistemomis turi būti realizuotos naudojant žiniatinklio paslaugas (angl. web-services), pagal W3C rekomendacijas. Žiniatinklio paslaugos bus realizuotos naudojant SOAP (angl. Simple Object Access Protocol), REST (angl. representational state transfer) ar kitą suderintą protokolą ir aprašytos WSDL (angl. Web Service Description Language) kalba.
      2. Sistemoje turi būti galimybė importuoti ir eksportuoti duomenis iš ir į Sistemą, naudojant aplikacijų programavimo sąsają (angl. application programming interface, API).
      3. Sistema turi palaikyti integracijų įvykių ir užklausų proceso saugią prieigą realiu laiku (autentifikavimas, sertifikavimas ir kt. ribojimai).
      4. Sistemoje naudojami duomenų apsikeitimai turi vykti realiu laiku.
      5. Detalios analizės ir projektavimo etapo metu su Užsakovu Tiekėjas aptars ir suderins integracijų įgyvendinimo būdus numatytiems reikalavimams pasiekti.
      6. Tiekėjas turi parengti kuriamos Sistemos integracijų sąsajų dokumentą, kuriame būtų pateikta:
         1. Integracijų diagramos;
         2. Būtinų sukurti sąsajų sąrašas;
         3. Spendimo architektūra;
         4. Duomenų srautai;
         5. Duomenų perdavimo / gavimo paslaugoms įgyvendinti naudojami standartai ir technologijos;
         6. Aprašyti veiklos scenarijai arba taikymo atvejai ir duomenų perdavimo taisyklės, apibrėžtos duomenų perdavimo / gavimo apimtys;
         7. Informacija apie naudojamas perduodamų / gaunamų duomenų saugumo užtikrinimo priemones;
         8. Apibrėžtas perduodamų / gaunamų duomenų formatas (užklausos, atsakymai, laukų kodai su aprašymais, klaidų kodai su aprašymais), aprašyti laukų atributai (tipas, aprašymas), pateikti visų užklausų ir atsakymų žinučių pavyzdžiai.
      7. Jeigu integracijos veikimui reikalingos papildomos sistemos licencijos, tai Tiekėjas turi nusimatyti šias licencijas.
      8. Kvalifikuotas elektroninis parašas turi būti realizuotas pačioje sistemoje arba per integraciją (web servisą) su Užsakovo naudojama išorine pasirašymo sistema.
   4. **Reikalavimai Naudotojo sąsajai:**
      1. Turi būti užtikrinamas Sistemos prieinamumas ne mažiau kaip 98 proc. laiko darbo dienomis nuo 7.00 val. iki 21.00 val.
      2. Sistema turi palaikyti UTF8 ir lietuvių kalbos abėcėlės rašmenis. Grafinė Sistemos sąsaja turi būti pritaikyta lietuvių ir anglų kalboms.
      3. Sistemoje pateikiamą informaciją gali matyti ir veiksmus atlikti tik autentifikavęsi naudotojai.
      4. Sistemoje autorizavimo mechanizmas turi būti realizuotas remiantis rolių modeliu (angl. Role-based Model) ir valdomas centralizuotai.
      5. Sistemoje turi būti galimybė naudotojams priskirti, keisti ir šalinti roles bei priskirti, keisti ir šalinti rolėms priskirtus prieigos teisių sąrašus.
      6. Sistemoje turi būti galimybė tvarkyti roles bei jų prieigos teises. Pakeitus esamų rolių teises, šios turi būti realiu laiku pritaikomos naudotojams, kuriems priskirta su pakeitimu susijusi rolė.
      7. Sistemoje turi būti galimybė kurti naujas roles.
      8. Sistemoje turi būti galimybė naudotojui priskirti daugiau nei vieną rolę.
      9. Sistemoje naudotojas turi galėti peržiūrėti tik tokią informaciją ir naudotis tik tokiomis funkcijomis, kurios yra nustatytos priėjimo teisėmis, pvz., jei Sistemoje naudotojas nori peržiūrėti informaciją, kuri yra nepriskirta jo rolei, Sistema turi rodyti pranešimą naudotojui, kad jis neturi prieigos prie informacijos teisės ir kitais būdais apriboti informacijos peržiūrą.
      10. Sistemoje turi būti galimybė eksportuoti naudotojų sąrašą su jų rolėmis ir teisėmis.
      11. Sistema turi atitikti sesijos valdymo reikalavimus. Privalomas funkcionalumas HTTPS sesijos apsaugai:
          1. Apsaugoti lankytojo / naudotojo visą sesiją SSL (nežemesnė kaip 1.3 versija), TLS pagalba;
          2. Neįtraukti sesijos ID į URL adresą arba nesiųsti jo siunčiamos užklausos antraštėje (angl. Referrer header);
          3. Užtikrinti, kad sesijos ID yra ilgas, sudėtingas, sugeneruotas iš atsitiktinių skaičių ir negali būti lengvai atspėjamas;
          4. Draudžiama saugoti sesijos ID;
          5. Sesijos ID turi būti šifruojamas ne mažesniu kaip 128 bitų ilgio raktu;
          6. Išvalomas sesijos objektas naudotojui išsiregistravus arba sesijai nustojus galioti.
      12. Sistemos naudotojui neatliekant veiksmų ilgiau kaip 30 minučių, pasijungimo sesija automatiškai turi būti uždaryta (angl. „logged off“).
      13. Vidinėje Sistemoje turi būti realizuotas vieno prisijungimo į sistemą (angl. Single Sign-On, SSO) sprendimas.
      14. Prieigos teisių valdymui turi būti galimybė sukonfigūruoti kelių veiksnių autentifikavimą (angl. multi-factor authentification).
      15. Sistemoje turi būti galimybė nustatyti naudotojų darbo sesijų trukmę ir užtikrinti sesijų uždarymą, kai sesija užimta ir / ar Sistema nenaudojama nustatytą laiką. Neveikimo laiko trukmė turės būti suderinta Projekto metu.
      16. Naudotojo sąsaja turi būti realizuota WEB technologijų pagrindu ir būti pasiekiama per naudotojo darbo vietoje įdiegtą interneto naršyklę.
      17. Naudotojo sąsaja turi būti pritaikyta naudojimuisi mobiliaisiais įrenginiais (Android ir iOS) ir palaikyti "responsive design".
      18. Sistemos naudotojo sąsajos turi būti suderinamos su šiomis naršyklėmis:
          1. Microsoft Edge (iki Sistemos naudojimo etapo pradžios vėliausios išleistos versijos);
          2. Google Chrome (iki Sistemos naudojimo etapo pradžios vėliausios išleistos versijos).
      19. Sistemos naudotojo sąsajose klaidų indikacija turi būti pateikiama šalia klaidą sukėlusio elemento (pvz., turi būti pažymėti laukai su klaidingai įvestais duomenimis).
      20. Sistema turi užtikrinti korektišką klaidų, kurias sukėlė neteisingi naudotojo veiksmai, valdymą. Sistemos naudotojui atlikus neteisingą (neleidžiamą) komandą arba nekorektiškai įvedus duomenis, Sistema turi naudotojui rodyti atitinkamus pranešimus ir po to grįžti į darbo būklę.
      21. Sistemoje turi būti užtikrinta, jog langų ir laukų išdėstymas užtikrintų visos reikšmingos informacijos matomumą ir pasiekiamumą viename ekrane.
   5. **Sistemos saugos reikalavimai**
      1. Sistema turi būti saugoma kriptuotoje saugykloje.
      2. Turi būti užtikrinamas šifravimo raktų (angl. "cipher keys“) saugumas. Šifravimo raktų ilgis turi būti ne mažesnis kaip 256 bitai.
      3. Tiekėjas privalo užtikrinti, kad diegiama Sistema būtų suderinama su Microsoft Defender ir ESET antivirusine programine įranga bei pažangiomis saugumo priemonėmis, tokiomis kaip EDR (Endpoint Detection and Response) ir XDR (Extended Detection and Response). Suderinamumas turi būti užtikrintas:
         1. darbo vietų aplinkoje (naudotojų kompiuteriuose, nešiojamuosiuose kompiuteriuose ir pan.);
         2. tarnybinėse stotyse (serveriuose), kuriose Sistema bus diegiama ar eksploatuojama.
      4. Tiekėjas turi užtikrinti, kad Sistema netrukdytų saugumo sprendimų (pvz., antivirusinė programinė įranga) veikimui ir atvirkščiai.
      5. Tiekėjas turi nurodyti ar reikalingi papildomi nustatymai bei išimtys (angl. exclusions) antivirusinėje ar EDR/XDR sistemoje, kad būtų užtikrintas tinkamas Sistemos veikimas.
      6. Sistemoje jautri ir (ar) konfidenciali informacija, neturi turėti galimybės būti dešifruota iš išorės.
      7. Sistema turi būti suderinama su Microsoft Information Protection (MIP) sprendimu ir palaikyti saugos žymų (angl. sensitivity labels) taikymą bei valdymą pagal organizacijos saugumo politiką.
      8. Sistema turi palaikyti dokumentų, pažymėtų Microsoft Information Protection saugos žymomis, įkėlimą, saugojimą, peržiūrą ir atsisiuntimą. Tai apima:
         1. apsaugotų (encrypted) dokumentų įkėlimą į sistemą;
         2. standartinę dokumentų peržiūrą (pvz., atidarymą naršyklėje ar peržiūros lange);
         3. greitąją peržiūrą (preview), kai dokumentas atvaizduojamas be pilno atidarymo, išlaikant saugos žymos apribojimus.
      9. Sistemoje turi būti numatyta galimybė nustatyti saugumo žymas siunčiamam laiškui ir dokumentui. Naudotojams turi būti suteikta prieigos teisė pakeisti standartinę saugumo žymą.
      10. Turi būti realizuotas teisių ir rolių priskyrimo naudotojams mechanizmas, leidžiantis kontroliuoti naudotojų prieigą prie Sistemos.
      11. Tiekėjas turės atlikti reikiamus Sistemos programavimo ir / ar konfigūravimo darbus, atsižvelgiant į Užsakovo arba techninio palaikymo Tiekėjo atstovų atliktą atsparumo įsilaužimams testavimo rezultatų ataskaitą ir ištaisyti aptiktas saugos spragas savo sąskaita.
      12. Turi būti realizuotas funkcionalumas, leidžiantis užtikrinti, kad Sistemos duomenys ir teikiamos funkcijos yra pasiekiamos tik autentifikuotiems naudotojams.
      13. Sistema turi užtikrinti, kad naudojama tik unikalius naudotojų identifikatorius / prisijungimo vardus. Sistema turi užtikrinti duomenų konfidencialumą, t. y. kad tik autentiški naudotojai gali registruotis sistemoje ir pasiekti tik jiems skirtus duomenis / funkcionalumą.
      14. Tiekėjas įsipareigoja laikytis gerųjų programinės įrangos kūrimo saugumo praktikų.
      15. Tiekėjas atlieka programavimo darbų analizę ir testavimą, atitinkantį sistemos saugumo reikalavimus ir gerąsias programinės įrangos saugumo praktikas:
          1. CWE/SANS 25 dažniausios programavimo klaidos (naujausia versija;
          2. The Center for Internet Security, Inc. (CIS®). Rekomendacijomis pateiktomis <https://downloads.cisecurity.org/#/> ;
          3. Sistema turi būti diegiama ir modifikuojama vadovaujantis naujausiomis ir geriausiomis saugumo praktikomis, galiojančiomis diegimo metu, tokiomis kaip CIS Controls (https://www.cisecurity.org/controls), taip pat atsižvelgiant į pasaulinės nepriklausomos organizacijos OWASP (angl. Open Web Application Security Project) TOP 10 išvardintų žinomų (kritinių) WEB pažeidžiamumų sąrašą bei OWASP teikiamas rekomendacijas (<http://www.owasp.org>).
      16. Sistemos naudotojo kompiuteryje (darbo vietoje) neturi būti instaliuojami jokie Sistemos komponentai (pvz. add-in, JAVA ir pan.), išskyrus naudotojo kompiuteryje gali būti instaliuojamas papildomas bendrinis programinis komponentas, jei toks programinis komponentas pasiūlomas įdiegti jungiantis prie Sistemos, nereikalaujantis papildomo licencijų įsigijimo ar nesukelia įsipareigojimo Užsakovui mokėti naudojimo mokesčius, jo įdiegimas nereikalauja specialių žinių, ir jei toks programinis komponentas nebuvo įdiegtas anksčiau.
      17. Tiekėjas. turi užtikrinti, kad Sistemos ir su ja susijusių paslaugų kūrime ir teikime būtų naudojama tik leistina ir licencijuota aparatinė ir programinė įranga.
      18. Sistemoje slaptažodžiai negali būti saugomi atviru tekstu.
      19. Sistema turi būti apsaugota nuo nesankcionuotos prieigos.
      20. Jeigu yra galimybė pasiekti elektroninius dokumentus ir kitus failus ne per Sistemos naudotojo sąsają (pvz. failai kurie saugomi sistemos failinėje struktūroje ar duomenų bazėje), tai failai turi būti apsaugoti arba užšifruoti.
      21. Sistema turi užtikrinti veikimą naudojantis HTTPS saugiu protokolu, sistemos programinė įranga duomenų perdavimui tarp Sistemos naudotojo kliento darbo vietos ir sistemos tarnybinės stoties privalo naudoti šifruotą ryšio kanalą. Ryšio kanalo šifravimui turi būti naudojama TLS (TLS 1.3 ar aukštesnė versija).
      22. Sistema turi užtikrinti pilną duomenų šifravimą (angl. end-to-end encryption), t. y. duomenys turi būti šifruojami perdavimo metu tarp paslaugos ir naudotojų kompiuterių metu, bei duomenų bazėse, tarnybinėse stotyse ir atsarginėse kopijose.
      23. Visi kiti sistemoms komponentai (kurie naudojami kaip pagalbiniai Sistemoje) turi būti naudojami pasitelkiant naujausią gamintojų programinę įrangą ir jei gamintojai teikia – turinčios ilgalaikį jos palaikymą (angl. long-term support (LTS)). Gamintojui išleidus naujesnę versiją – ji turi būti ištestuota ir sudiegta ne vėliau kaip per 6 mėnesius po išleidimo datos.
      24. Sistemoje neturi būti jokių paslėptų, saugumą silpninančių funkcijų, įskaitant: kenksmingos programinės įrangos, virusų, „kirminų“, „laiko minų“, neautorizuotų prieigų ar funkcijų (Trojans, backdoors, easter eggs). Reikalavimui įgyvendinti gali būti pasitelktas ir atsakingas subteikėjas (gamintojas), pvz., jei pasitelkiamas subteikėjas (gamintojas), Paslaugų Teikėjas gali būti atsakingas už modifikacijų saugumą, subteikėjas (gamintojas) – standartinį sprendimą.
      25. Tiekėjas garantinio ir techninio palaikymo metu turi informuoti Užsakovą apie Sistemos programinės įrangos ir jos komponentų gamintojų išleistus saugumo pažeidžiamumų pataisymus.
      26. Sistemos pažeidžiamumai (angl. vulnerabilities) yra tikėtini – programinėje įrangoje bus klaidų, dalis kurių gali turėti įtakos sistemos saugumui. Užsakovas ir Tiekėjas skirs deramas pastangas, kad identifikuotų silpnas saugumo vietas ar pažeidžiamumus kuo ankstesniame Sistemos vystymo ciklo etape.
      27. Tiekėjas sužinojęs apie galimas sistemos saugumo spragas ar silpnas vietas, šią informaciją Užsakovui pateiks nedelsiant ir pilnoje apimtyje.
      28. Tiekėjas vykdo periodinis saugos atnaujinimų diegimą, remiantis CVE kritiškumo lygiu.

|  |  |  |
| --- | --- | --- |
| **Lygis** | **Maksimalus laikas pašalinimui** | |
|  | **Iš interneto pasiekiamiems pažeidžiamumams** | **Iš vidinio tinklo pasiekiamiems pažeidžiamumams** |
| Kritinis | 2 dienas | 2 dienos |
| Aukštas | 7 dienos | 30 dienų |
| Vidutinis | 30 dienų | 90 dienų |
| Žemas | 180 dienų | 360 dienų |

* + 1. Nesant galimybei atnaujinimų sudiegti pagal CVE laikų lentelę, turi būti informuotas Užsakovas, įvertintos rizikos ir suderinti kiti įgyvendinimo laikai.
    2. Sistemoje turi būti užtikrintos priėjimo prie Sistemos apsaugos priemonės nuo kenkėjiškų programų atakų, pvz., įsilaužimo prevencijos sistema (angl. Intrusion Prevention System (IPS)) / įsilaužimo stebėjimo sistema (angl. Intrusion detection system (IDS)) , ugniasienė.
    3. Integracijoms ir duomenų mainams su kitomis sistemomis turi būti naudojamas saugus WEB Service:
       1. ne žemesnis kaip WS\* arba alternatyvus;
       2. apsaugotas slaptažodžiu;
       3. naudojamas saugus protokolas HTTPS;
       4. šifruojamas duomenų perdavimo kanalas, naudojant TLS 1.3 ar aukštesnė versiją.

Tikslus sąrašas bus suderintas sistemos diegimo metu su paslaugų teikėju.

* + 1. Sistemoje turi būti užtikrintas atsarginio kopijavimo sistemos veikimas, kad sistemos atkūrimas tenkintų tokius reikalavimus (reikalavimas taikomas Sistemos darbo aplinkai):
       1. Atkūrimo laikas (angl. Recovery Time Objective (RTO)) neviršytų 8 val.
       2. Būtų atkurti ne senesni nei 24 val. duomenys (angl. Recovery Point Objective (RPO)), t. y., turi būti užtikrintas atsarginio kopijavimo atlikimas kas 24 val. ir atsarginių duomenų kopijų saugojimas.
    2. Sistemoje turi būti galimybė daryti rezervines kopijas visiems saugomiems duomenims, tenkinant Sistemos numatytus greitaveikos reikalavimus ir netrikdant darbo su Sistema.
    3. Atkūrus duomenis turi būti atliekamas duomenų atkūrimo kokybės patikrinimas, norint įsitikinti ar buvo išlaikytas duomenų teisingumas ir vientisumas.
    4. Sistemoje turi būti galimybė atkurti jos būseną į ankstesnę (point-in-time-restore).
    5. Numatyti Sistemos naudotojai turi galėti lengvai peržiūrėti konkrečių audito įrašų informaciją (tiek ekraninėje formoje, tiek ataskaitoje).
    6. Sistemoje turi būti galimybė apsaugoti audito įrašus nuo nesankcionuoto ar netyčinio pakeitimo, pvz., Sistemos naudotojui peržiūrint audito įrašo informaciją, neturi būti galima pakeisti įrašo.
    7. Sistemos administratoriams turi būti panaikinta galimybė ištrinti ar redaguoti administratoriaus veiksmų žurnalinius įrašus
    8. Sistemos audito įrašai negali būti redaguojami ar kitaip keičiami.
    9. Informacinėje sistemoje turi būti registruojama, su galimybe realiu laiku eksportuoti ir / ar perduoti į centralizuotą žurnalinių įrašų kaupimo sistemą (angl. "SIEM"), ir ne mažiau kaip 6 mėnesius išsaugoma saugumo ir kitų įvykių informacija tokia kaip:
       1. prisijungusio naudotojo ar administratoriaus identifikatoriai;
       2. įvykių laikai;
       3. įvykių registravimo funkcijos įjungimas / išjungimas;
       4. įvykių trynimas, kūrimas ir (ar) keitimas;
       5. kompiuterio, iš kurio jungiamasi, informacija;
       6. sėkmingos ir nesėkmingos prieigos įrašai;
       7. administratoriaus teisių naudojimas;
       8. prieigos teisių pokyčiai;
       9. integracijų žurnaliniai įrašai;
       10. sistemos konfigūracijos keitimas, sisteminių priemonių naudojimas;
       11. resursai, prie kurių buvo suteikta prieiga;
       12. sisteminiai pranešimai;
       13. informacija apie veiksmus su naudotojais.

Tikslus sąrašas bus suderintas sistemos diegimo metu su Užsakovu.

* + 1. Tiekėjo darbuotojų darbo priemonėse privalo būti įdiegta ir veikti  galiojanti, patikimo gamintojo antivirusinė sistema.
    2. Tiekėjas įsipareigoja neatskleisti administruojamų duomenų, neperleisti tretiesiems asmenims ir užtikrintą kokybišką jų apsaugą.
    3. Tiekėjas įsipareigoja, jog visa archyvinė informacija, Sutarties galiojimo laikotarpiu bus apsaugota nuo trečiųjų šalių ir pasibaigus sutarčiai nemokamai ir saugiai perduota pirkėjui suderintu formatu.
    4. Po Sutarties nutrūkimo tarp Tiekėjo ir Užsakovo, Tiekėjas privalo iš savo Sistemos pašalinti visus sukauptus archyvinius duomenis, jų visas galimas kopijas ir neperduoti jų tretiesiems asmenims.
    5. Apie bet kokius galimus duomenų pasisavinimo ar nutekėjimo atvejus, Tiekėjas nedelsdamas privalo informuoti Užsakovą ir imtis visų įmanomų priemonių, situacijai suvaldyti.
    6. Tiekėja turi užtikrinti galimybę Užsakovui ne rečiau kaip vieną kartą per metus atlikti Tiekėjo kontrolę, patikrą su tikslu įvertinti Tiekėjo taikomas informacijos saugos užtikrinimo organizacines bei technines priemones.
    7. Užsakovui pareikalavus, Tiekėjas pateiks patvirtinimą - deklaraciją, kad kūrimo ir vystymo darbai atitinka 5.5.15 punkte keliamus reikalavimus.
    8. Tiekėjas kartu su Užsakovu detalizuos saugumo reikalavimus vystymo darbams, Identifikuotų rizikų pagrindu.
    9. Tiekėjas turi naudoti konfigūracijų valdymo sistemą kuri autentifikuoja sistemos kūrime dalyvaujančius Tiekėjo darbuotojus ir registruoja jų veiksmus.
  1. **Reikalavimai Asmens duomenų apsaugai:**
     1. **Reikalavimai dėl atitikties Bendrajam duomenų apsaugos reglamentui**
        1. Tiekėjas ir (arba) kitos Šalys, veikiantys kaip duomenų tvarkytojai ir tvarkantys Užsakovo asmens duomenis, turi įgyvendinti technines ir organizacines priemones, kad apsaugotų Užsakovo duomenis pagal BDAR reikalavimus, užtikrinant, be kita ko, atitikimą pritaikytosios duomenų apsaugos (data protection by design) ir standartizuotosios duomenų apsaugos (data protection by default) (BDAR 25 str.) įskaitant, bet ne apsiribojant saugojimo terminų nustatymą, asmens duomenų trynimą ar anonimizavimą automatizuotomis priemonėmis. Tiekėjas turi pateikti visų Šalių, tvarkančių Užsakovo asmens duomenis, aukščiau nurodytų reikalavimų įgyvendinimo įrodymus Užsakovui.
        2. Tiekėjas po Sutarties pasirašymo nedelsiant turi su Užsakovu sudaryti duomenų tvarkymo susitarimą (DTS), pagal Užsakovo pateiktą DTS formą. Tais atvejais, kai Užsakovo asmens duomenis tvarkys kita Šalis, Paslaugos teikėjas turi užtikrinti, kad kita Šalis su Užsakovu sudarys DTS pagal Užsakovo pateiktą DTS formą. Pagrįstai atvejais, kai nėra galimybės sudaryti DTS pagal Užsakovo pateiktą formą, Tiekėjas turi užtikrinti, kad duomenų tvarkytojo paslaugų teikimo sąlygose, be kita ko, būtų įtrauktos pagal BDAR 28 str. 3 d. privalomos nuostatos.
        3. Užsakovas turi būti nedelsiant informuojamas apie Sistemos informacijos ir kibernetinės saugos įvykius ir incidentus ar asmens duomenų saugumo pažeidimus, jų įtaką Užsakovo informacijos ir duomenų saugumui bei jų valdymo būklę. Užsakovas turi turėti galimybę susisiekti su saugos įvykius ir incidentus valdančiais asmenimis, kad įsitikintų valdymo proceso efektyvumu.
        4. Produktai (sistemos) ir (arba) paslaugos turi būti sukonfigūruotos taip, kad leistų Užsakovui įgyvendinti BDAR numatytas duomenų subjektų teises: teisę būti informuotam apie duomenų tvarkymą, teisę susipažinti su asmens duomenimis, teisę reikalauti ištaisyti duomenis, teisę būti pamirštam, teisę apriboti duomenų tvarkymą, teisę nesutikti su duomenų tvarkymu, teisę į duomenų perkeliamumą (BDAR III skyrius). Užsakovo Tiekėjui perduoti duomenų subjektų prašymai neturi būti papildomai apmokestinami.
        5. Sistema turi atitikti asmens duomenų apsaugos principus ir nuostatas kaip aprašyta Europos parlamento ir Tarybos Reglamente 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau BDAR, Bendrasis duomenų apsaugos reglamentas).
        6. Tiekėjas turi užtikrinti, kad Užsakovo duomenys nebus perduodami už Europos ekonominės erdvės ribų, nebent egzistuotų bent viena iš BDAR V skyriuje numatytų perdavimo už Europos ekonominės erdvės ribojimo išimčių.
     2. Asmens duomenų saugumo užtikrinimas:
        1. Sistemoje turi būti galimybė tvarkyti asmens duomenis tik tiems specialistams, kuriems yra suteiktos atitinkamos rolės ir prieigos teisės;
        2. Sistemoje turi būti galimybė automatiniu būdu pagal nustatytas taisykles, kai tai neprieštarauja nustatytiems teisės aktams ir vidinėms tvarkoms, nuasmeninti visus arba konkrečius pasirinkto asmens ar asmenų grupės asmeninius duomenis. Atliekant funkciją, turi būti išlaikomas duomenų vientisumas;
        3. Sistemoje turi būti galimybė automatiniu būdu parengti tvarkomų asmens duomenų išrašą pagal pasirinktą asmenį (darbuotoją, subkontraktorių, kt.);
        4. Sistemoje administratoriui turi būti galimybė šalinti pasirinktus jautrius ir (ar) konfidencialius duomenis, kurių nėra privaloma kaupti / kurie nėra reikalingi tolimesniam sėkmingam Sistemos darbui (pvz., asmeninę naudotojų informaciją);
        5. Sistemoje turi būti galimybė tvarkyti asmens duomenų saugojimo terminus ir suėjus įstatymų ar vidinių tvarkų nustatytam terminui automatiniu būdu ištrinti asmens duomenis.

1. **IT Paslaugų valdymo (ITSM) platforma ir kreipiniai**
   1. IT paslaugų valdymo (ITSM) platforma:
      1. Kreipinių registravimui Tiekėjas turi turėti IT Paslaugų valdymo (ITSM) platformą (toliau ITSM).
      2. Tiekėjo ITSM turi suteikti galimybes registruoti kreipinius įvairiais nurodytais kanalais: elektroniniu paštu; fiksuoto ir mobilaus ryšio telefonu; naudojant WEB sąsają.
      3. Tiekėjas turi būti įdiegęs veikiančius ir aprašytus incidentų bei keitimų valdymo procesus, atitinkančius IT paslaugų valdymo (ITIL ar lygiavertės metodikos) gerųjų praktikų rekomendacijas bei veikiantį internetinį portalą kreipiniams registruoti bei peržiūrėti.
      4. Tiekėjo ITSM turi užtikrinti operatyvų atgalinį ryšį ir informacijos apie incidentus realiu laiku (angl. On-line) teikimą interneto tinklalapyje, veikiančiame HTTPS protokolu.
      5. ITSM turi informuoti apie užregistruotų incidentų būklę, planuojamą incidentų išsprendimo datą ir laiką bei incidentų išsprendimą.
   2. Sprendimą, kokio tipo klaida yra nustatyta, priima Užsakovo paskirti atsakingi asmenys, suderinę su Teikėjo paskirtais atsakingais asmenimis.
   3. Tiekėjas privalo išanalizuoti klaidą, pateikti Užsakovui klaidų šalinimo įgyvendinimo būdo aprašymą pagal tokius grafikus:
      1. kritinės klaidos atveju: ne vėliau kaip per 2 darbo valandas nuo Užsakovo pranešimo pateikimo momento;
      2. nekritinės klaidos atveju: ne vėliau kaip per 8 darbo valandas nuo Užsakovo pranešimo pateikimo momento.
   4. Klaidų šalinimo terminai derinami su Užsakovu, tačiau turi būti ne ilgesni kaip (terminas pradedamas skaičiuoti nuo informavimo apie klaidą pateikimo Tiekėjui momento):
      1. kritinės klaidos atveju: ne vėliau kaip per 1 darbo dieną nuo Užsakovo pranešimo pateikimo momento;
      2. nekritinės klaidos atveju: ne vėliau kaip per 2 darbo dienas nuo Užsakovo pranešimo pateikimo momento.
   5. Tiekėjas su Užsakovu raštu gali susiderinti kitus, Užsakovui priimtinus, klaidų pašalinimo terminus.
   6. Bendravimo bei dokumentavimo kalba teikiant paslaugas turi būti lietuvių kalba.
2. **Reikalavimai pateiktims ir dokumentacijai**
   1. Visa dokumentacija turi būti parengta elektroninėje formoje laikantis bendrinės lietuvių kalbos taisyklių. Dokumentacija, kurioje nėra aprašomi veiklos procesai ir funkcijos (diegimo ar administravimo instrukcijos ir pan.), gali būti rengiama anglų kalba.
   2. Rengiant Sistemos dokumentaciją, turi būti laikomasi bendrųjų dokumentacijos rengimo reikalavimų: turi būti išlaikyta vienoda dokumentų struktūra ir stilius, jei aprašomo objekto specifika nereikalauja kitokio aprašymo būdo; visos naudojamos sąvokos ir žymėjimai turi būti paaiškinti „žodynėlyje“; dokumentacijoje naudojamos sąvokos ir žymėjimai turi turėti tą pačią prasmę visose vietose, kuriose jie naudojami; dokumentacija turi būti rengiama ir Sistemos diegimas turi būti vykdomas vadovaujantis valstybės informacinių sistemų kūrimą reglamentuojančiais Lietuvos Respublikos teisės aktais.
   3. Visi Tiekėjo parengti dokumentai turės būti suderinti su Užsakovu. Detalūs dokumentų derinimo principai turės būti pateikti ir suderinti Tiekėjo parengtame Paslaugų teikimo reglamente.
   4. Tiekėjas yra atsakingas už dokumentuose pateiktos informacijos teisingumą ir aktualumą bei reguliarų šių dokumentų atnaujinimą ir naujų versijų pateikimą.
   5. Dokumentų pokyčiai turi būti kontroliuojami. T. y.:
      1. Dokumentas privalo turėti priskirtą versijos numerį;
      2. Dokumentas privalo turėti versijų pokyčių registracijos lentelę (kas, kada ir kodėl sukūrė naujos versijos dokumentą).
   6. Kiekvieno etapo pabaigoje turi būti pateikiama etapo ataskaita bei etapo rezultatai.
   7. Pateiktys privalo apimti šiuos rezultatus, pateikiamus atitinkamų informacinės sistemos gyvavimo ciklo stadijų metu:
      1. Paslaugų teikimo reglamentą
      2. Projekto planą ir grafiką
      3. Sistemos analizės dokumentas, kuris apima:
         1. Sistemos specifikaciją;
         2. Sistemos projektavimą;
         3. Sistemos architektūrą;
         4. Sistemos standartines funkcijas;
         5. Sistemos plėtros funkcijas;
         6. Sistemos veiklos procesų aprašą.
      4. Testavimo planą
      5. Testavimo scenarijus
      6. Testavimų ataskaitą
      7. Bandomosios eksploatacijos planą, kuriame turi būti pateikta bandomosios eksploatacijos metodika (eiga, klaidų stebėjimas, bandomosios eksploatacijos pabaigos kriterijai), įvedimo į bandomąją eksploataciją ir bandomosios eksploatacijos veiklų grafiką
      8. Bandomosios eksploatacijos ataskaitą
      9. Mokymų planą ir mokymų medžiagą
      10. Sistemos diegimo – atstatymo planą
      11. Informacinės sistemos eksploatacinę dokumentaciją turi sudaryti:
          1. Bendro sistemos aprašymo dokumentas, kuris turi apimti:
             1. Sistemos tikslą;
             2. Aprašyti sistemos funkcijas;
             3. Aprašyti aukšto lygio sistemos architektūrą.
          2. Sistemos architektūros dokumentas, kuris turi:
             1. Būti tiek detalus, kad iš jo būtų galima suprasti pagrindinę sistemos sprendimo idėją ir patį sprendimą;
             2. Įvardinti ir parašyti visus vidinius sistemos komponentus ir integracijas su kitomis sistemomis;
             3. Paaiškinti sistemos komponentų išdėstymą ir jų sąsajas;
             4. Paaiškinti duomenų srautus;
             5. Pateikti sistemos integracijos sąsajos (API) aprašymą (tiek funkcinį, tiek ir administravimo).
          3. Sistemos administravimo ir priežiūros vadovas, kuris turi apimti:
             1. Aprašyti administratoriaus operacijų ir priežiūros procesus taip, kad juos būtų galima atlikti be rangovo įsitraukimo;
             2. Aprašyti tikėtinas klaidas ir incidentus, sutrikimus ir pateikti sprendimo instrukcijas;
             3. Aprašyti neautomatizuotas procedūras;
             4. Aprašyti pagrindinių žurnalų (log) įrašų tipus, kur juos rasti ir kaip interpretuoti.
      12. Sistemos saugumo reikalavimai
      13. Įdiegimo instrukcija
      14. Sistemos atkūrimo instrukcija
      15. Naudotojo vadovas, kuriame matytųsi funkcijų medis ir jų aprašymai. Aprašymai turi būti išsamūs ir suprantami naudotojui savarankiškai vykdant konkrečias užduotis, apimti visas numatytas sistemos funkcijas, iliustruoti naudotojo sąsajos ekranvaizdžiais.
      16. Garantinio aptarnavimo bei naudotojų konsultavimo reglamentas
      17. Sistemos diegimo priėmimo–perdavimo aktas.
      18. Sistemos Techninio palaikymo priėmimo–perdavimo aktas.
      19. Vystymo paslaugų priėmimo–perdavimo aktas elektronine forma po kiekvieno užsakymo įvykdymo.
   8. Bandomosios eksploatacijos ir garantinio aptarnavimo metu paaiškėjus, kad vadovuose, instrukcijose pateikta informacija nėra išsami (neaprašyti arba netiksliai aprašyti įprasti Sistemos naudojimo, administravimo bei konfigūravimo veiksmai), Tiekėjas, be papildomo užmokesčio, privalo konsultuoti Užsakovo paskirtus darbuotojus instrukcijose neaprašytais klausimais, patikslinti instrukcijas ir pateikti Užsakovui atnaujintas jų versijas.
   9. Projekto ir Sistemos dokumentai turi būti aiškūs ir vienareikšmiškai suprantami. Projekto ir sistemos dokumentuose neturi būti nereikalingų ar pasikartojančių tekstų, į aktualias susijusių dokumentų sritis turi būti teikiamos nuorodos (o ne kartojamas tekstas).
   10. Neapsiribojant šioje Techninėje specifikacijoje reikalaujamais dokumentais Tiekėjas savo nuožiūra gali pateikti ir kitą papildomą dokumentaciją, jeigu yra toks poreikis.
   11. Naudojamos trečiųjų šalių papildomos programinės įrangos, reikalingos Sistemos veikimui, kuri nėra įtraukta į pagrindinę Sistemos kainą, sąrašas, apimantis:
       1. programinės įrangos pavadinimą ir gamintoją;
       2. licencijos tipą (pvz., vienkartinė, metinė, prenumerata, nemokama ir pan.);
       3. licencijos galiojimo terminą (jei taikoma).
3. **Reikalavimai mokymams (ne mažiau kaip 20 val.):**
   1. Tiekėjas turės apmokyti Užsakovo darbuotojus naudotis Sistema. Naudotojai turi būti mokomi Sistemos naudojimo pagrindų ir paruošiami tolesniam savarankiškam mokymuisi, siekiant visiškai įsisavinti Sistemos naudojimo atvejus.
   2. Paslaugų teikėjas praveda Sistemos mokymus Užsakovo darbuotojams, dalyvaujantiems Sistemos priėmimo testavime.
   3. Mokymai turi būti atlikti iki Sistemos bandomosios eksploatacijos pradžios.
   4. Tiekėjas su Užsakovu turi suderinti mokymuose dalyvaujančių asmenų skaičių ir nurodyti tai mokymų plane.
   5. Tiekėjas yra atsakingas už mokymo medžiagos ir mokymų plano paruošimą bei mokymų pravedimą.
   6. Pagal mokymų plane suderintą procedūrą ir tvarką turi būti apmokyti būsimi Sistemos naudotojai, duomenų tvarkytojai ir administratoriai.
   7. Mokymai turi būti vykdomi testavimo ar kitoje specialiai mokymams Tiekėjo parengtoje aplinkoje, kurios konfigūracija turi atitikti gamybinę aplinką;
   8. Įdiegus Sistemą, Užsakovui turi būti pateikti elektronine forma Sistemos naudotojo ir Sistemos administravimo vadovai.
   9. Sistemos naudotojams turi būti pateikiamos vizualinės pagalbos priemonės padedančios greičiau išmokti naudotis Sistemos – „Žingsnis po žingsnio“ stiliaus vadovai ir vaizdo įrašai su tekstiniais ar garso komentarais, kuriuose pateikiami atskiros užduotys, suskaidytos pagal atliekamus procesas ir / ar naudotojo roles. Tiekėjas gali pasiūlyti kitus lygiaverčius vizualinės pagalbos priemonių sprendimus, apimančius aukščiau nurodytus atvejus.
   10. Vadovai turi būti atnaujinami atliekant Sistemoje naujinimus / pakeitimus ateityje.
4. **SUTARTINIŲ ĮSIPAREIGOJIMŲ VYKDYMO VIETA**
   1. Gudelių g. 49, Vilnius.
   2. Laisvės pr. 10, LT-04215 Vilnius.
   3. Kita: Nuotoliniu būdu, Europos Ekonominės erdvės (EEE) teritorijoje.
5. **BAUDOS IR DELSPINIGIAI**
   1. Pardavėjui nesilaikant terminų, nustatytų Techninės specifikacijos 6.4 punkte, taikoma bauda – 5 (penki) Eur už kiekvieną pradelstą valandą (valanda laikoma pradelsta pilna valanda. Pvz., Užsakovas vėluoja sureaguoti 15, 30 arba 45 minutes – tai 5 (penkių) Eur bauda už šį laiką taikoma nebus. Jei Paslaugos teikėjas vėluoja sureaguoti 2 valandas 15 minučių – bus taikoma 10 (dešimties) Eur bauda už pavėluotas pilnas 2 valandas).