

TECHNINĖ SPECIFIKACIJA

1. SĄVOKOS IR SUTRUMPINIMAI

- 1.1. Pirkėjas** – AB „Energijos skirstymo operatorius“
- 1.2. Tiekėjas arba Vykdytojas** – ūkio subjektas – fizinis asmuo, privatusis juridinis asmuo, viešasis juridinis asmuo, kitos organizacijos ir jų padaliniai ar tokių asmenų grupė, su kuriuo Pirkėjas sudaro Sutartį.
- 1.3. Sutartis** – Sutartis, sudaroma tarp Tiekėjo ir Pirkėjo dėl Pirkimo objekto.
- 1.4. Paslaugos** – programinės įrangos techninio aptarnavimo ir vystymo paslaugos.
- 1.5. Techninio aptarnavimo (TA) paslaugos** – Programinės įrangos klaidų šalinimas, problemų sprendimas, palaikymo darbai ir konsultavimas.
- 1.6. Plėtimo paslaugos (PP)** – Pirkėjo pageidaujamos paslaugos, reikalingos PĮ funkcionalumo praplėtimui ar pakeitimui. Plėtimo paslaugų užsakymas bus fiksuojamas pasirašant Paslaugų užsakymo aktą (4 priedas), o atlikimas bus fiksuojamas pasirašant Paslaugų priėmimo-perdavimo aktą (3 priedas). Vystymo paslaugas sudaro Programinės įrangos funkcionalumo keitimas, papildoma duomenų analizė – tai Pirkėjo duomenų analizė, kuri susijusi su Pirkėjo duomenų nagrinėjimu, siekiant surasti ir išsiaiškinti vartotojo klaidas, arba pateiktų situacijų modeliavimu, siekiant patenkinti papildomus Pirkėjo poreikius, taip pat yra traktuojama kaip plėtimo paslaugos.
- 1.7. Programinė įranga (PI)** – Vykdytojiui prižiūrėti perduota programinė įranga, apibrėžiama kaip Pirkėjo aplinkoje įdiegta programinė įranga, Vykdytojo pritaikyta Pirkėjo poreikiams, t.y., modifikuotos ir parametrizuotos pagal Pirkėjo reikalavimus, įskaitant papildomus Pirkėjo pakeitimus, kuriuos Tiekėjas atliko.

2. PIRKIMO OBJEKTAS

Telemetrijos programinės įrangos „TEMEKA“ palaikymo ir vystymo paslaugos.

3. PIRKIMO OBJEKTO APIMTYS

Paslaugų preliminarus darbo valandų skaičius metams – 267 val. Perkančioji organizacija įsipareigoja pirkti 15 val. paslaugų per mėnesį. Kitą paslaugų kiekį pirs pagal poreikį ir neįsipareigoja išpirkti viso paslaugų kiekio. Telemetrijos sistemos vystymo, funkcionalumo plėtimo, modifikavimo ir kitos papildomos techninio aptarnavimo paslaugos bus perkamos pagal poreikį.

4. SUTARTINIŲ ĮSIPAREIGOJIMŲ VYKDYMO VIETA

Vilnius, Aguonų g. 24;

Vilnius, Motorų g. 2.

5. REIKALAVIMAI PIRKIMO OBJEKTUI

5.1. Esamos situacijos aprašymas

Telemetrinė sistema skirta surinkti informaciją iš dujų reguliavimo punktų, dujų vartotojų apskaitos punktų, katodinės apsaugos stočių telemetrinių posistemių. Norint, kad sistema veiktų tinkamai būtinos telemetrijos programinės įrangos palaikymo paslaugos.

5.2. Pirkimo objekto aprašymas

Pateikiamas priede Nr. 1 – Techninė specifikacija – Objekto aprašymas.

Bendriniai saugumo reikalavimai pateikti priede Nr. 2.

6. PRIEDAI

Priedas Nr. 1 – Techninė specifikacija

Priedas Nr. 2 – Bendriniai saugumo reikalavimai

TECHNINĖ SPECIFIKACIJA - OBJEKTO APRAŠYMAS

1. ĮVADINĖ INFORMACIJA

1.1. Perkamos paslaugos, susijusios su AB „Energijos skirstymo operatorius“ (toliau – Pirkėjas) eksploatuojamos skirstomųjų dujotiekių telemetrijos sistemos (reguliavimo punktų telemetrijos posistemės, dujų vartotojų apskaitos telemetrijos posistemės, katodinės apsaugos telemetrijos posistemės ir magistralinio dujotiekio SCADA duomenų bazės) (toliau – Sistema) techniniu aptarnavimu, sistemos vystymu (funkcionalumo plėtimu) (toliau – Paslaugos).

1.2. Paslaugos apima Sistemos:

- Techninį aptarnavimą;
- taikomosios programinės įrangos klaidų šalinimą;
- taikomosios programinės įrangos vystymą (funkcionalumo plėtimą, programinės įrangos modifikavimą, esamų funkcionalumo tobulinimą ir kt.)
- taikomosios programinės įrangos diegimo, konfigūravimo, konsultavimo bei kitos paslaugos pagal „Techninėje specifikacijoje“ nurodytus reikalavimus.

1.3. Taikomosios programinės įrangos modulių vystymo bei modernizavimo paslaugos bus atliekamos atskirais užsakymais. Numatoma, kad vystymo ir modernizavimo programavimo paslaugos bus užsakomos pagal AB „Energijos skirstymo operatorius“ poreikius ir atitinkamai įformintas užsakymo užduotis, paslaugų terminai bus suderinti su paslaugų tiekėju.

1.4. Paslaugos turi būti tiekiamos adresu: Vilnius, Aguonų g. 24, Motorų g. 2.

2. EKSPLOATUOJAMOS SKIRSTOMŲJŲ DUJOTIEKIŲ TELEMETRIJOS SISTEMOS FUNKCIONALUMAS

2.1. Sistemos paskirtis:

Telemetrinė sistema skirta surinkti informaciją iš dujų reguliavimo punktų, dujų vartotojų apskaitos punktų, katodinės apsaugos stočių telemetrinių posistemų.

2.2. Sistemos programinė ir sisteminė aplinka. Telemetrijos sistema realizuota daugiasluoksnės architektūros principu. Duomenų bazių serverių operacinė sistema yra naudojama Microsoft Windows 2008 Server ir duomenų bazių valdymo sistema yra naudojama Oracle Database 11g Release 2.

2.3. Telemetrijos sistema per WEB servisus keičiasi duomenimis su perdavimo sistemos operatoriaus programine įranga.

2.4. Programinės įrangos funkcijos:

2.4.1. Telemetrijos informacijos duomenų bazių formavimas, kaupimas, duomenų klasterizacija, rezervavimas.

2.4.2 Informacijos priėmimas/perdavimas iš/į RTU kontrolerį per GSM mobilųjį tinklą (interfeisas RS 232) ir TCP/IP tinklą (interfeisas Ethernet 10/100 Tbase).

2.4.3. Priimtose iš RTU informacijos atvaizdavimas ir peržiūrėjimas grafiniame ir tekstiniame režime.

2.4.4. Informacijos išvedimas į spausdinimo įrenginius.

2.4.5. Informacijos nuskaitymo iš RTU kontrolerio vykdymo protokolas.

2.4.6. Avarinių signalų, gautų iš RTU kontrolerio, kontrolė, protokolavimas, priėmimo patvirtinimo perdavimas.

2.4.7. Informacijos surinkimo iš RTU kontrolerio periodiškumo valdymas, nuskaitymo laiko nustatymas, nuskaitymo laiko intervalų nustatymas.

2.4.8. Objektų valdymo informacijos perdavimas į RTU.

2.4.9. Kontroliuojamų taškų parametrų skaitinių reikšmių atvaizdavimas ekrane stebimos stoties technologinėje struktūrinėje schemoje

2.4.10. Objekto technologinės schemos redagavimas, naujų schemų kūrimas.

2.4.11. Dujotiekio bendros struktūros atvaizdavimas, pažymint stebimus objektus ir jų darbinės būsenas (viskas normos ribose, avarinis pranešimas ir panašiai). Galimybė pasižymėjus schemoje stotį, išsikviesti parametrų ir pranešimų sąrašus, stoties struktūrą. Detalesnis patikslinimas bus pateiktas darbo eigoje.

2.4.12. Dujotiekio bendros struktūrinės schemos, atskirų technologinių schemų, pažymėtų atskiru dalių vaizdo padidėjimas monitorių ekranuose, keičiant vaizdo mastelį (zoom funkcija).

2.4.13. Reikalingų parametrų reikšmių statistika, kitimas dienos, savaitės, mėnesio ir pan. laikotarpyje.

2.4.14. Grafinis reikšmių atvaizdavimas (pagal 6 punktą). Iki 10 skirtingų kreivių viename grafike.

2.4.15. Dviejų koordinatinių markeris grafiko reikšmių indikavimui, intervalo tarp dviejų pozicijų toje pačioje kreivėje reikšmių nustatymui, intervalo tarp dviejų pozicijų skirtingose kreivėse reikšmių nustatymui ir t. t.

2.4.16. Grafiko dalies padidėjimo funkcija, perskaičiuojant ašių mastelius pagal padidinto grafiko dydį (zoom funkcija).

2.4.17. Valdomų sklendžių padėtis, galimybė keisti padėtį įvedus slaptažodį.

2.4.18. Dujų sunaudojimo skaitiklių (tame tarpe ir iš mechaninių skaitiklių į RTU priimtas ir suskaičiuotas impulsų skaičius) reikšmių momentinis atvaizdavimas, statistika, grafinis atvaizdavimas.

2.4.19. Kontroliuojamų stočių aprašymas (techniniai pasai) (stoties tipas, vieta, struktūra, kontroliuojami ir valdomi parametrai, leistinos parametrų kitimo ribos, duomenų nuskaitymo periodiškumas, GSM modemo telefono numeris, dujų srauto skaitiklių tipas, kitos įrangos tipai, įrangos patikros terminai su automatine terminų priminimo funkcija, kiti reikalingi parametrai).

2.4.20. Informacijos nuskaitymo iš RTU protokolai, pažymint nuskaitymo (ar bandymo nuskaityti) datą, laiką, rezultatą (pavyko nuskaityti ar ne), nenuskaitymo priežastį, modemo diagnostika, ryšio praradimo priežastys, klaidų duomenyse fakto identifikavimas. Turi būti realizuota atskiras informacijos nuskaitymo iš RTU sąrašas (pateikiamas ekrane dispečeriui) apie objektus iš kurių nepavyko nuskaityti informacijos (nenuskaitymo intervalo trukmė turi būti administruojama) tam tikrą laiką. Šie objektai turi būti atžymėti dujotiekio bendroje schemoje pakeičiant objekto spalvą.

2.4.21. Turi būti automatinis ir paprastas informacijos nuskaitymo iš RTU kontrolerių režimai. Automatinis režimas pagal nustatytą objektų apklausos eiliškumo sąrašą ir užduotą pradinį nuskaitymo pradžios laiką ir nuskaitymo intervalą automatiškai vykdo periodinį informacijos surinkimą iš RTU. Paprastame režime informacijos nuskaitymas iš RTU vykdomas nuskaitydamas vieną kartą išrinktų objektų RTU tuo momentu, kada tai atliekama (nuskaitymas vienkartinis, neperiodinis).

2.4.22. Turi būti realaus laiko "on-line" informacijos nuskaitymo iš RTU kontrolerių režimas. Šiame režime informacijos nuskaitymas iš RTU vykdomas susijungiant ir nuskaitydamas išrinkto objekto RTU iki ryšio nutraukimo momento (inicijuojamas iš dispečerio pusės). Duomenys atvaizduojami objekto technologinėje schemoje, pagal poreikį turi būti išvedama reikšmių lentelė ir grafikas. Šiame režime turi būti modemo darbo kontrolė, kuri užtikrintų automatinį modemo atjungimą nesant stebėtojo darbo požymių. "On-line" režimas turi turėti aukštesnį prioritetą už automatinį duomenų nuskaitymą.

2.4.23. Avarinių pranešimų protokolai, nurodant priežastį (būtinai nurodant datą, laiką, stoties pavadinimą).

2.4.24. Avariniai pranešimai turi būti perduoti į visus dispečerinės darbo vietų kompiuterius. Patvirtinus pranešimą bet kurioje dispečerinės darbo vietoje, avarinis pranešimas turi būti nuimamas iš visų dispečerinės darbo vietų monitorių ekranų.

2.4.25. Avarinis pranešimas dispečerinės darbo vietoje turi būti gerai matomas ekrane (visiškas priėmimo ir atvaizdavimo prioritetas) ir palydimas kompiuterio garso signalu. Kartu su avariniu pranešimu (tuo pačiu duomenų nuskaitymu) turi būti perduotos momentinės objekto parametrų reikšmės. Signalas ir vaizdas gali būti "nugesintas" tik peržiūrėjus informaciją ir duomenų bazėje (pranešimų protokole) įrašius personalo, kuris priėmė ir peržiūrėjo pranešimą, duomenis. Avariniai pranešimai turi būti perduoti vienu metu į visas dispečerinės darbo vietas. Vienoje, bet kurioje dispečerinės darbo vietoje patvirtinus pranešimą, pranešimas turi būti nuimtas. Be personalo duomenų fiksavimo pranešimas negali būti patvirtintas.

2.4.25.1. Avariniai pranešimai tai:

- Slėgio (įėjimo, išėjimo) ribų pažeidimas (du lygiai: perspėjimo ir avarinis);
- Atkirtos vožtuvų suveikimas;
- Temperatūros ribų pažeidimas (du lygiai: perspėjimo ir avarinis);
- Dujų apskaitos prietaisų avariniai pranešimai;
- Apsaugos sistemos daviklių informacija (priešgaisrinės, apsaugos, perimetrinės);
- Uždujinimo kontrolės sistemos;
- Elektros maitinimo pažeidimas;
- Katodinės stoties išėjimo įtampos išsijungimas;
- UPS sistemos pranešimas.
- Informacijos perdavimo priemonių (ryšio) signalizacija;
- Pašalinio vartotojo kreipimasis į RTU per modemą (neatitinka slaptažodis, telefono numeris ir pan.).

Turi būti numatyta avarinių pranešimų svarbos ir patvirtinimo būtinumo konfigūravimo funkcija.

2.4.26. Avarinio signalo patvirtinimo fakto perdavimas į RTU kontrolerį.

2.4.27. Atvaizduojamo parametro reikšmės atvaizdavimo spalva (tiek grafikuose, tiek skaitinė reikšmė) turėtų keistis priklausomai nuo to kokiose ribose parametras yra (pvz. normos ribose – žalias, virš normos ribų raudonas, artėjant prie kritinių ribų ($\pm 10 - 20 \%$) – geltonas ir pan.).

2.4.28. Galimybė keisti kontroliuojamų parametrų kitimo ribas, kritines reikšmes.

2.4.29. RTU ir ryšio įrangos darbingumo kontrolė (RTU maitinimo sistemos kontrolė, RTU testas, modemo darbingumo kontrolė).

2.4.30. Bet kurioje darbo vietoje turi būti galima gauti tą pačią informaciją vienu metu.

2.4.31. Bet kurios informacijos, esančios bet kurios darbo vietos bet kurio kompiuterio monitoriaus ekrane perdavimas ir atvaizdavimas projekciniame ekrane (projekcinis ekranas valdomas iš atskiro valdymo modulio, kuris įjungtas į bendrą SCADA LAN). Programinė įranga turi užtikrinti nepriklausomą vienas nuo kito atskirų darbo vietos kompiuterių informacijos atvaizdavimą į projekcinį ekraną tuo pačiu metu. Tiekėjas privalo suderinti savo programinę įrangą su projekcinio ekrano valdymo įranga. Jeigu reikalinga turi būti rašomos tam tikslui reikalingos taikomosios programos.

2.4.32. Programinė įranga turi užtikrinti papildomų duomenų įvedimą rankiniu būdu į technologinių schemų langus ir į duomenų bazę (iš objektų, kuriuose nėra automatinio nuskaitymo arba parametrai, kurie negali būti nuskaityti automatiškai).

2.4.33. Programinė įranga užtikrina vartotojų ir slaptažodžių valdymą.

2.4.34. Programinė įranga leidžia spausdinti ataskaitas.

3. NAUDOJAMA SISTEMINĖ PROGRAMINĖ ĮRANGA

3.1. Pirkėjas Telemetrijos sistemos eksploatavimui naudoja šią turimą sisteminę, duomenų bazių valdymo sistemų (DBVS) programinę įrangą:

- MS Windows 2008 R2 Enterprise x64;- Oracle Database 11g Release 2;

4. REIKALAVIMAI SISTEMOS TECHNINIO APTARNAVIMO PASLAUGOMS

4.1. Užtikrinti Sistemos techninį aptarnavimą, užtikrinant naudojamos Sistemos funkcionavimą ir Sistemos techninį palaikymą.

4.2. Teikti konsultacinę pagalbą Pirkėjo Sistemos naudotojams ar kitiems paskirtiems Pirkėjo darbuotojams, sprendžiant iškilusias problemines situacijas (telefonu ir elektroniniu paštu).

4.3. Pirkėjo darbuotojai visas problemas, susijusias su Sistema, turi turėti galimybę registruoti pagalbos sistemoje tiesiogiai, arba siunčiant elektroninį laišką, arba telefonu. Sistemos vartotojui, užregistravus problemą pagalbos sistemoje, turi būti atsiųstas elektroninis patvirtinimo laiškas, kur kiekvienai problemai būtų suteiktas unikalus identifikavimo numeris.

4.4. Teikti konsultacijas telefonu iškart, atsakymus, reikalaujančius papildomos analizės, pateikti per 8 darbo val.

4.5. Teikti konsultacijas elektroniniu paštu, atsakymus pateikiant per 8 darbo val.

4.6. Iškylus kritinėms problemoms, kurios įtakoja Sistemos veikimą, reakcijos laikas į registruotą Pirkėjo kreipinį turi būti ne daugiau kaip 4 (keturios) darbo valandos.

4.7. Identifikuotos programinės įrangos ir paslaugų klaidos turi būti ištaisytos 2 savaičių laikotarpyje po jų užregistravimo (arba kitokiu būdu užfiksavimo) dienos.

4.8. Po Pirkėjo užsakymo ir paramos teikimo tvarkos susitarimo, Šalių suderintais terminais Tiekėjas suteikia Pirkėjui paramą darbo vietoje.

4.9. Tais atvejais, kai gedimo neįmanoma likviduoti per Sutartyje nustatytą gedimų pašalinimo laiką, Vykdytojas apie tai informuoja Pirkėją ir gedimo šalinimas vykdomas abipusiu šalių susitarimu.

4.10. Užtikrinti esamos programinės įrangos atliktų pakeitimų klaidų ir netikslumų, kurie neatitinka esamos sistemos funkcinių reikalavimų dokumentų, taisymą.

4.11. Apmokyti Sistemos naudotojus darbui su Sistema, įvertinant atliktus Sistemoje pakeitimus ir atnaujinimus.

4.12. Sistemos techninis aptarnavimas turi apimti ir naujų funkcijų sukūrimą bei esamų praplėtimą ir įdiegimą.

4.13. Sistemos tobulinimo bei funkcionalumo plėtimo darbai atliekami raštu suderinus su Pirkėjo atstovu paslaugų turinį, apimtį ir terminus. Funkcionalumo plėtimo bei Sistemos modifikavimo/tobulinimo darbai galės būti atliekami tik gavus raštišką Pirkėjo atstovo patvirtinimą.

5. REIKALAVIMAI SISTEMOS VYSTYMO (FUNKCIONALUMO PLĖTIMO) PASLAUGOMS

5.1. Bendrieji reikalavimai:

5.1.1. Visos paslaugos, kurios sudaro Sistemos vystymo (funkcionalumo plėtimo) objektą, turi būti vykdomos laikantis duomenų saugą reglamentuojančių teisės aktų.

5.1.2. Sistemos programinė įranga turi būti praplečiama ir keičiama:

- laikantis modulinio principo, užtikrinant sistemos vientisumą, lengvas plėtimo galimybes;
- remiantis daugiasluoksnės architektūros principu.

5.1.3. Tiekėjas pradeda teikti Sistemos vystymo, funkcionalumo plėtimo ir techninio aptarnavimo paslaugas ne vėliau kaip per 5 d. d. po Pirkėjo užsakymo pateikimo.

5.1.4. Užsakomos Sistemos vystymo, funkcionalumo plėtimo ir techninio aptarnavimo paslaugos turi būti atliktos per Pirkėjo nustatytą ir su tiekėju suderintą laiko tarpą.

5.1.5. Visais atvejais Sistemos vystymo, funkcionalumo plėtimo ir papildomų techninio aptarnavimo paslaugų užsakymų vykdymo metu naujai sukurta ar pakeista programinė įranga Tiekėjas gali perduoti AB „Energijos skirstymo operatorius“ specialistams, tik pilnai ją ištestavęs ir įsitikinęs, kad ją įdiegus „gamybinėje“ aplinkoje, nebus sutrikdytas tos Sistemos ar kitų taikomųjų sistemų darbas ir visi įdiegti pakeitimai veiks taip, kaip buvo numatyta užsakyme ir kituose dokumentuose, nustatančiuose funkcinius reikalavimus kuriamai ar keičiamai programinei įrangai.

5.1.6. Sprendimą dėl Sistemos vystymo bei funkcionalumo plėtimo užsakymų vykdymo metu naujai sukurtos ar pakeistos programinės įrangos diegimo gamybinėje aplinkoje priima sutartyje nurodytas Pirkėjo atsakingas atstovas už Sistemos techninį aptarnavimą.

5.2. Sistemos vystymo ir funkcionalumo plėtimo (modernizavimo) paslaugos apima:

5.2.1. Telemetrijos sistemos taikomosios programinės įrangos ir duomenų bazės pakeitimų ar naujo funkcionalumo kūrimą;

5.2.2. Telemetrijos sistemos integracinių sąsajų su kitomis AB „Energijos skirstymo operatorius“ ar kitų šalių taikomosiomis sistemomis keitimą bei kūrimą;

5.2.3. Telemetrijos sistemos integracijos su kitomis sistemomis pakeitimų derinimą su AB „Energijos skirstymo operatorius“ nurodytais tiekėjais;

5.2.4. Telemetrijos sistemos naudojimosi patogumo gerinimą;

5.2.5. Programos kodo ir duomenų bazių užklausų optimizavimą;

5.2.6. Telemetrijos sistemos perkėlimą į naujas aplinkas naujai suinstaliuojant programinę įrangą bei sukonfigūruojant aplinką.

5.3. Telemetrijos sistemos vystymo bei modernizavimo paslaugos užsakomos pagal AB „Energijos skirstymo operatorius“ poreikius ir atitinkamai įformintas užsakymo užduotis.

5.4. Plėtimo paslaugų užsakymas bus fiksuojamas pasirašant Paslaugų užsakymo aktą (4 priedas), o atlikimas bus fiksuojamas pasirašant Paslaugų priėmimo-perdavimo aktą (3 priedas).

5.5. Už Sistemos funkcionalumo plėtimo, modifikavimo, konsultavimo ir kitas technines priežiūros paslaugas, nenumatytas sutarties 5 priede, Pirkėjas sumoka pagal valandinį įkainį nurodytą Sutartyje.

6. BENDRIEJI REIKALAVIMAI

6.1. Tiekėjas ryšiams su Pirkėju skiria atstovus, kurių kontaktinė informacija pateikiama Sutarties SD Priede Nr. 2. Tiekėjo atstovas atsakingas už visų kontaktų ir darbų su Pirkėju koordinavimą ir vykdymą.

6.2. Visos Tiekėjo atliktos paslaugos fiksuojamos Paslaugų priėmimo-perdavimo akte, kurio forma nurodyta 3 priede. Tiekėjo ir Pirkėjo pasirašytas Paslaugų priėmimo-perdavimo aktas yra pagrindas PVM sąskaitai faktūrai išrašyti už papildomas apmokamas paslaugas, atliktus šios Sutarties galiojimo metu.

6.3. Tiekėjas įsipareigoja teikti Pirkėjui gamintojo rekomendacijas Sistemos eksploatavimo ir modernizavimo klausimais, informuojant apie naują programinę įrangą bei įrangos išplėtimus.

6.4. Pirkėjas įsipareigoja laikytis gamintojo rekomendacijų saugios Sistemos ir Programinės įrangos eksploatacijos klausimais. Pirkėjas įsipareigoja ne vėliau kaip prieš 3 (tris) darbo dienas raštu informuoti Tiekėją apie bet kokius savarankiškai ar trečiųjų šalių numatomus atlikti naujos kompiuterinės ar programinės įrangos instaliavimo ar tinklo plėtimo darbus.

6.5. Šiame punkte Šalys programinę įrangą supranta bet kokią kompiuterinę programą arba bylų visumą, keičiančią operacines sistemos arba kitų programų bylas (sistemines bylas, registrus, šablonus ar panašiai).

Priedas Nr. 2 prie Techninės specifikacijos
BENDRINIAI SAUGUMO REIKALAVIMAI

I. Bendriniai saugumo reikalavimai Paslaugų teikėjui:

1. Paslaugų teikėjo informacijos saugumas **turi būti valdomas** vadovaujantis ISO 27001 (arba lygiavėrio) ir ISO 27002 (arba lygiavėrio) informacijos saugumo valdymo standartais. Toliau tekste pateikiami reikalavimai, sąvokos ir terminai suprantami taip, kaip nurodoma minėtuose standartuose.
2. Paslaugų teikėjas, ne rečiau kaip vieną kartą per vienerius metus, turi atlikti informacinio saugumo **rizikų vertinimą**, apimančį visas teikiamas paslaugas. Visoms rizikoms kurių lygis yra nepriimtinas turi būti parengtas ir įmonės vadovybės patvirtintas rizikų valdymo **priemonių planas**. Rizikų vertinimo metodika, rizikų vertinimo ataskaita, rizikų priimtino lygis ir rizikos valdymo priemonių planas siejamas su perkama/prižiūrima paslauga/sistema turi būti suderinti su Klientu.
3. Atlikti dujų telemetrijos sistemos priežiūra gali tik sankcionuotas personalas. Sankcionuotas personalas – tai personalas, kurį patvirtino ESO Prevencijos skyrius.
4. Paslaugų teikėjas turi turėti patvirtintą ir iškomunikuotą informacijos **saugumo politiką**.
5. Paslaugų teikėjo darbuotojai turi būti **supažindinti** su informacijos saugos politika ir **ja vadovautis**.
6. Paslaugų teikėjas turi turėti paskirtą už **informacijos saugą atsakingą** asmenį.
7. Paslaugų teikėjas turi turėti paskirtą **informacijos saugos auditorių**, kuris negali būti atsakingas ir už informacijos saugumo priemonių įgyvendinimą, t.y. kontrolės ir sistemos priežiūros funkcijos turi būti atskirtos.
8. Paslaugų teikėjas turi turėti patvirtintą **informacijos valdymo** (klasifikavimo, žymėjimo ir naudojimo) tvarką, apimančią reikalavimus Kliento informacijai.
9. Paslaugų teikėjo darbuotojai, kuriems suteikiama prieiga prie Kliento informacijos, privalo pasirašyti **konfidencialumo susitarimus**, o darbuotojai, turintys administratoriaus teises – papildomus įsipareigojimus. Susitarimų ir įsipareigojimų dokumentų projektai turi būti suderinti su Klientu.
10. Paslaugų teikėjo darbuotojų informacijos **saugumo žinių lygis** turi būti nustatytas ir periodiškai **vertinamas**.
11. Paslaugų teikėjas turi turėti parengtas **elektroninio pašto, interneto, kompiuterio** ir kitų informacinių išteklių **naudojimo instrukcijas**, taikomas Paslaugų teikėjo darbuotojams, kuriose nurodytos leistino naudojimo ribos.
12. Paslaugų teikėjas turi turėti patvirtintus **fizinės saugos politiką** ir planus, užtikrinančius tinkamą, informacinių išteklių, kuriuose saugoma Kliento informacija, fizinę apsaugą.
13. Paslaugų teikėjas turi turėti patvirtintą saugaus informacijos **laikmenų utilizavimo tvarką**.
14. Paslaugų teikėjas turi turėti formalizuotus **keitimų ir konfigūracijų valdymo tvarkas ir procesus**, apimančius ir teikiamas Klientui paslaugas, užtikrinančius Sistemos pakeitimų planavimą, registravimą ir klasifikavimą, įtakos vertinimą, tvirtinimą, testavimą, vykdymą, atstatymą ir informavimą. Darbuotojai privalo vadovautis šiomis tvarkomis.
15. Kliento informacija Paslaugų teikėjo nešiojamuose kompiuteriuose, mobiliuose įrenginiuose ir laikmenose turi būti saugoma **užšifruota**.
16. Paslaugų teikėjas turi turėti patvirtintą saugumo **incidentų valdymo tvarką**, apimančią ir teikiamas Paslaugas.
17. Paslaugų teikėjas turi turėti patvirtintą ir ištestuotą Paslaugų teikėjo **veiklos tęstinumo valdymo planą**, apimančį ir Klientui teikiamų Paslaugų tęstinumą. Planas turi būti periodiškai išbandomas, rezultatai dokumentuojami.
18. Paslaugų teikėjo informacijos saugumo valdymo sistema (**ISVS**), rizikų valdymo priemonės ir Klientui teikiamos Paslaugos turi būti kasmet vertinama **nepriklausomų auditorių**. Atitikties vertinimo išvada pateikiama Klientui.

19. Šie **reikalavimai ne mažesne apimtimi taikomi** visoms Paslaugų teikėjo subrangos organizacijoms, jeigu šios subrangos organizacijos, Kliento raštišku sutikimu, turi ar gali įgyti prieigą prie Kliento duomenų ir/ar aplinkos.
20. Paslaugų teikėjas periodiškai kiekvieną mėnesį pateikia Klientui informaciją apie visas **subrangos organizacijas**, kurioms buvo perduota Kliento informacija (jei subranga buvo numatyta Paslaugų teikimo sutartyje).
21. Klientas turi teisę **audito** būdu įsitikinti, kad Paslaugų teikėjas laikosi šių reikalavimų.

II. Bendriniai saugumo reikalavimai perkamai (prižiūrimai) Sistemai (Paslaugai):

22. Naudotojų autentifikavimo (angl. *Identity*), autorizacijos (angl. *Access Management*) ir administravimo reikalavimai:

- 22.1. Paslaugų teikėjas prieigą prie Kliento informacijos turi suteikti tik tiems Kliento darbuotojams, kuriems ji būtina Paslaugų teikimui ir tik tokia apimtimi, kuri būtina pagal atliekamas darbo funkcijas, t.y. turi būti įgyvendintas **principas „būtina žinoti“** (t.y. suteikiama minimali, darbo užduočių atlikimui būtina informacija, prieigos teisės ir priemonės.). Tokių darbuotojų sąrašas turi būti patvirtintas Paslaugų teikėjo įmonės vadovo, pateiktas Klientui ir kartą per 1 mėn. peržiūrimas. Apie bet kokius pasikeitimus informuojamas Klientas.
- 22.2. Paslaugų teikėjo įmonėje turi būti **atskirtos prieigos teisių suteikimo atsakomybės**, t.y. poreikio inicijavimo, tvirtinimo ir atlikimo funkcijų negali atlikti vienas ir tas pats Paslaugų teikėjo asmuo, t.y. turi būti įgyvendintas **„funkcijų atskyrimo“ principas**.
- 22.3. Paslaugų teikėjas turi turėti parengtas vidines savo prieigos teisių prie informacinių sistemų vartotojams suteikimo, peržiūros, pakeitimo ir panaikinimo procedūras, kurios apibrėžia kaip ir kokiais pagrindais Paslaugų teikėjo darbuotojams suteikiama prieiga, kas atsakingas už prieigos patvirtinimą ir reikiamų pakeitimų įgyvendinimą. Procedūrose turi būti aprašyti Sistemos tipiniai vartotojų vaidmenys ir išimtinių teisių suteikimo tvarka. Ši dokumentacija turi būti suderinta su Klientu.
- 22.4. Turi būti realizuota galimybė prieigos teisės prie Sistemos suteikti tik pagal **principą „būtina žinoti“** (suteikiant prieigos teises/roles, nustatant reikiamą funkcionalumą, parenkant naudojamus sistemos modulius/formas/ataskaitas ir t.t.).
- 22.5. Sistema privalo turėti autorizacijos funkcionalumą, paremtą Kliento turima centralizuota vartotojų duomenų baze, užtikrinantį **centralizuotą vartotojų autentifikavimą** ir jiems priskirtų teisių/rolių suteikimą, panaikinimą ir kontrolę.
- 22.6. Vartotojų darbas Sistemoje **tik administratoriaus** teisėmis draudžiamas.
- 22.7. Paslaugų teikėjas turi turėti sistemos **administratorių prieigos valdymo tvarką**, kuri aiškiai identifikuotų administratorių roles, bei joms suteiktas teises, identifikuotų asmenis, gaunančius privilegijuotas teises ir jų panaudojimo paskirtį (tikslą).
- 22.8. Paslaugų teikėjas turi užtikrinti, kad Sistemoje norimu periodiškumu būtų galima **peržiūrėti privilegijuotų vartotojų veiksmus**, juos dokumentuoti, t.y. formuoti ataskaitas (detalizuota kituose punktuose).
- 22.9. Paslaugų teikėjas turi užtikrinti, kad Sistemoje galima įdiegti Kliento pateiktus reikalavimus **slaptažodžiams**, apibūrinančius naudojamų slaptažodžių ilgį, kompleksiskumą, neatspėjamumą ir kartotinumą. Šie reikalavimai apima ir naudotojams suteiktų slaptažodžių konfidencialumą, saugaus slaptažodžio perdavimą, naudotojo, kuriam perduodamas pirminis slaptažodis ar keičiamas slaptažodis, tapatybės nustatymą.
- 22.10. Pradiniai **gamintojų** įvesti slaptažodžiai Sistemoje turi būti pakeisti pagal bendrus slaptažodžiams keliamus reikalavimus ir perduoti Klientui.
- 22.11. **Slaptažodžiams** keliami reikalavimai:
- 22.11.1. slaptažodžiai privalo būti sudaryti iš mažųjų ir didžiųjų raidžių, skaičių ir/arba specialiųjų simbolių,
- 22.11.2. darbuotojų slaptažodis turi būti sudarytas iš mažiausiai 8 simbolių, **administratorių** slaptažodžiai privalo būti sudaryti iš mažiausiai 12 simbolių,

- 22.11.3. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pvz., gimimo data, šeimos narių vardai ir pan.),
- 22.11.4. slaptažodis privalo būti **reguliariai keičiamas**, t.y. ne rečiau kaip 90 dienų laikotarpyje, apie tai iš anksto informuojant vartotoją,
- 22.11.5. tarp pakartotinio slaptažodžio keitimo turi būti ne mažesnis kaip 24 val. laiko tarpas,
- 22.11.6. laikini arba **pradiniai** slaptažodžiai privalo būti sukurti atsitiktine tvarka ir unikalūs kiekvienam vartotojui,
- 22.11.7. laikini arba pradiniai slaptažodžiai privalo būti pakeisti **pirmo prisijungimo metu**,
- 22.11.8. slaptažodžiai negali būti naudojami tokie patys, kokie buvo naudoti 6 mėnesių laikotarpyje,
- 22.11.9. buvę 6 slaptažodžiai negali būti pakartotinai naudojami to pačio vartotojo,
- 22.11.10. didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius - 5 kartai,
- 22.11.11. sistemoje saugomi slaptažodžiai privalo būti užšifruoti. Šifravimui naudojamas vienpusio šifravimo algoritmas,
- 22.11.12. slaptažodžiai persiunčiami viešaisiais tinklais privalo būti papildomai apsaugoti (užšifruoti),
- 22.11.13. slaptažodžiai negali būti siunčiami toje pačioje žinutėje su vartotojo vardu,
- 22.11.14. užmiršti slaptažodžiai privalo būti pakeisti, nenaudojami pakartotinai,
- 22.11.15. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu (netaikoma tik naujų vartotojų laikiniams slaptažodžiams),
- 22.11.16. draudžiama slaptažodžius atskleisti tretiesiems asmenims,
- 22.11.17. draudžiama techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius - jie privalo būti pakeisti pagal nurodytus reikalavimus.
- 22.12. Paslaugų teikėjas turi užtikrinti, kad Sistema naudoja tik **unikalius vartotojų identifikatorius**, valdomus centralizuotai Kliento turimomis priemonėmis.
- 22.13. Paslaugų teikėjas turi užtikrinti duomenų **konfidencialumą** Sistemoje, t.y. kad **tik autentifikuoti vartotojai** gali registruotis Sistemoje ir pasiekti tik jam skirtus duomenis ar funkcionalumą.
- 22.14. Paslaugų teikėjas turi užtikrinti, kad **vienu metu ir tuo pačiu prisijungimo vardu** į Sistemą gali jungtis tik vienas autentifikuotas vartotojas.
- 22.15. Sistema (ar jos pagalbiniais sprendimais) turi leisti nustatyti ir automatiškai kontroliuoti įvestą vartotojui **galiojimo terminą**, po kurio vartotojo prisijungimas automatiškai blokuojamas.
- 22.16. **Administratorių slaptažodžiai ir vardai** Sistemoje turi būti saugomi vartotojų registre, su prieigos kontrolės užtikrinimu ir informacijos **šifravimu**.
- 22.17. Paslaugų teikėjas turi paskirti asmenį, **atsakingą už Sistemos administravimą** (priežiūrą). Paskirto asmens kontaktinę informaciją Paslaugų teikėjas turi pateikti Klientui. Apie bet kokią paskirto Sistemos administratoriaus pasikeitimą nedelsiant turi būti informuojamas Klientas.
- 22.18. Sistemoje kūrimo, testavimo ir gamybinės **aplinkos** privalo būti **atskirtos**.
- 22.19. Sistemos **testinėse aplinkose negali** būti naudojami **gamybiniai duomenys**, t.y. privalu naudoti netikrus arba iš gamybinių sistemų paimtus **pakeistus** / iškraipytus duomenis.
- 22.20. Jei Sistemos testinėje aplinkoje privalo būti naudojami gamybinių sistemų duomenys:
 - 22.20.1. prieiga prie šių testinių sistemų privalo būti apribota iki minimumo, o sąrašas suderintas su Klientu,
 - 22.20.2. testinėms aplinkoms privalo būti taikomi tokie patys saugos reikalavimai kaip ir gamybinėms aplinkoms,
 - 22.20.3. testinėje aplinkoje gamybinių sistemų duomenys po testavimo privalo būti nedelsiant ištrinti.
- 22.21. Sistemoje **draudžiama** naudoti **automatinį** elektroninių laiškų **persiuntimą** į ne Bendrovei priklausančias elektroninio pašto dėžutes.
- 22.22. Paslaugų teikėjas Klientui turi pateikti **dokumentuotą** kiekvienos Sistemos rolės ir teisės aprašą.

23. Žurnalinių įrašų (angl. log) kaupimo ir priežiūros reikalavimai

- 23.1. Paslaugų teikėjas turi užtikrinti, kad **Sistema turi žurnalinių įrašų** (angl. *Logs*) rinkimo, saugojimo ir **perdavimo** į kitas specializuotas žurnalinių įrašų surinkimo ir analizės sistemas (angl. *SIEM*) funkcionalumą.
- 23.2. Paslaugų teikėjas turi dokumentuoti ir pateikti Klientui žurnalinių įvykių **aprašą**.

- 23.3. Paslaugų teikėjo Sistema privalo **kaupti šiuos žurnalinius įvykius**:
- 23.3.1. sėkmingą ir/arba nesėkmingą prisijungimą,
 - 23.3.2. visus privilegijuotų vartotojų veiksmus,
 - 23.3.3. visus pakeitimus vartotojų teisėms ir prieigai,
 - 23.3.4. sisteminių objektų sukūrimą ir išvalymą,
 - 23.3.5. sistemos/aplikacijos išjungimą, paleidimą ar perkrovimą.
- 23.4. Žurnalinius įvykius sudaro:
- 23.4.1. įvykio tipas,
 - 23.4.2. vartotojo identifikatorius,
 - 23.4.3. įvykio data ir laikas,
 - 23.4.4. sėkmingos ir nesėkmingos prieigos įrašai,
 - 23.4.5. įvykio šaltinis,
 - 23.4.6. susiję sistemos komponentai ar resursai,
 - 23.4.7. tinklo adresas ir/arba naudotas protokolas.
- 23.5. Paslaugų teikėjas turi užtikrinti, kad Sistemoje renkami žurnaliniai įrašai **renkami** nefiltruota (angl. *non-filtered*) ir nenormalizuota (angl. *non-normalized*) forma ir **saugomi** ne trumpiau kaip **6 mėn.**.
- 23.6. Paslaugų teikėjas turi užtikrinti, kad Sistemoje kaupiami žurnaliniai įrašai yra **apsaugoti nuo nesankcionuoto pakeitimo**, o **prieiga** prie jų – **apribota** (tik skaitymo teisės Sistemos administratorių, įmonės auditorių ir pan. pareigybų prieigai).
- 23.7. Paslaugų teikėjo Sistema turi turėti galimybę (suderintu su Klientu periodiškumu ir formatu) **perduoti** Sistemos žurnalinius įrašus **į Kliento centralizuotą** žurnalinių įrašų surinkimo, saugojimo ir analizės sistemą (SIEM).

24. Reikalavimai rezervinių kopijų (angl. *Backup*) valdymui, duomenų archyvavimui, duomenų ir sistemos prieinamumo (angl. *Availability*) ir patikimumo (angl. *Reliability*) reikalavimai

- 24.1. Paslaugų teikėjas turi turėti dokumentuotą Sistemos konfigūracijos ir jos duomenų atsarginio kopijavimo procesą, užtikrinantį sutartinių įsipareigojimų su Klientu vykdymą (per suderintą su Klientu laiko tarpą atkurti sistemas ir jų duomenis).

25. Sistemos pažeidžiamumų (informacinės sistemos ar tinklo įrenginio netinkama apsauga nuo konkrečios grėsmės) valdymo ir atnaujinimo reikalavimai

- 25.1. Paslaugų teikėjas turi turėti formalizuotą **techninių pažeidžiamumų** (angl. *Vulnerability*) valdymo procesą, numatantį informacinės sistemos pažeidžiamumų testavimą iki įvedant ją į eksploataciją, identifikuojantį atsakingus asmenis, bei jiems paskirtas atitinkamas funkcijas. Tvarka turi apimti proceso vertinimo ir gerinimo, pažeidžiamumų stebėjimo ir vertinimo, pataisymų diegimo veiksmus, identifiкуotus IT komponentus, kurių pažeidžiamumai nuolatos būtų vertinami, apibrėžtas aptiktų pažeidžiamumų kategorizavimo ir prioritetizavimo gaires, nustatytus reagavimo į pažeidžiamumus terminus ir veiksmus, numatytą periodinę atliktų veiksmų patikrą.
- 25.2. Paslaugų teikėjas ne rečiau kaip **vieną kartą per mėn.** Sistemos infrastruktūrai ir jos komponentams turi vykdyti **pažeidžiamumo skenavimą** (angl. *vulnerability scan*), o saugumo ir kritinius atnaujinimus (angl. *security update*) įdiegti:
- 25.2.1. **kritiniai** pažeidžiamumai (kuriems yra priskirti 9-10 balų pagal tarptautinę CVSS klasifikavimo skalę <https://web.nvd.nist.gov/view/vuln/search>) privalo būti įdiegti **per 30 dienų** nuo pažeidžiamumo identifikavimo dienos,
 - 25.2.2. **svarbūs** pažeidžiamumai (kuriems yra priskirti 6-8 balai pagal tarptautinę CVSS klasifikavimo skalę <https://web.nvd.nist.gov/view/vuln/search>) privalo būti įdiegti **per 90 dienų** nuo pažeidžiamumo identifikavimo dienos,
 - 25.2.3. **kiti** pažeidžiamumai privalo būti įdiegti **per 360 dienų** nuo pažeidžiamumo identifikavimo dienos.
- 25.3. Apie pažeidžiamumų **patikros rezultatus** ir atliekamus atnaujinimo veiksmus ne rečiau kaip **vieną kartą per mėnesį** raštiškai (elektronine forma) Paslaugų teikėjas turi informuoti Klientą.

26. Saugumo reikalavimai prieigai per mobiliuosius įrenginius

- 26.1. Mobiliuose įrenginiuose (mobilūs telefonai, planšetiniai kompiuteriai) turi būti įdiegtos šios apsaugos priemonės:
 - 26.1.1. Įdiegtas MDM (angl. Mobile device management) sprendimas (organizacijos ir asmeninės duomenų saugojimo erdvės atskyrimas, duomenų šifravimas, „baltieji“ programinės įrangos sąrašai, slaptažodžių/PIN politika)
 - 26.1.2. Įdiegta Kliento antivirusinė programinė įranga
 - 26.1.3. Įdiegta Kliento nuotolinės prieigos (VPN) programinė įranga

27. Reikalavimai kompiuterizuotai vartotojo darbo vietai (KDV)

- 27.1. Kompiuterizuotai darbo vietai (KDV) bus taikomi Kliento reikalavimai (Active directory security policies) ir be local administrators suteiktų teisių.

28. Ataskaitų rengimas, peržiūra ir valdymas, dokumentacija

- 28.1. Paslaugų teikėjo Sistema turi turėti galimybę suformuoti norimo periodo **žurnalinių įrašų** apibendrintas ir detalias ataskaitas (angl. *reports*) ir jas pateikti Kliento atsakingiems asmenims.
- 28.2. Paslaugų teikėjo Sistema turi turėti galimybę suformuoti periodinę ataskaitą apie visas Sistemos **vartotojų turimas prieigas** ir jų **teises/roles** (prieigos teisių matrica).
- 28.3. Paslaugų teikėjo Sistema turi turėti galimybę peržiūrėti **prisijungimų prie Sistemos** ataskaitas, kuriose turi būti matoma iš kokio IP adreso, kuriuo laiku ir koks darbuotojas jungėsi, kokie buvo atliekami veiksmai (pvz., turinio redagavimas/šalinimas, laiškų siuntimas, naujų naudotojų sukūrimai ar teisių/rolių jiems keitimas ir pan.).
- 28.4. Paslaugų teikėjo Sistema turi turėti galimybę suformuoti periodinę (vieną kartą per mėn.) ataskaitą apie Sistemos **sistemonių ir administratorių paskyrų** (angl. *accounts*) **veiksmus**.

29. Saugumo reikalavimai, keliami informacinės sistemos priežiūrai

- 29.1. Paslaugų teikėjas Klientui turi pateikti Sistemos pakeitimo testavimo scenarijų ir gautus testavimo rezultatus. Testavimas turi būti atliekamas tik testinėje aplinkoje.
- 29.2. Testavimo rezultatuose Paslaugų teikėjas turi dokumentuoti ir pateikti Klientui testavimo scenarijus ir jų rezultatus, kuriuose nurodyta:
 - 29.2.1. testuojama funkcija (reikalavimai),
 - 29.2.2. kokie veiksmai turi būti atlikti iki testavimo ir kokie pradiniai duomenys reikalingi testavimui,
 - 29.2.3. kokius veiksmus reikia atlikti testavimo metu su testiniais duomenimis,
 - 29.2.4. koks rezultatas yra laukiamas, kokie gauti rezultatai/duomenys tai patvirtina,
 - 29.2.5. testuotojo išvada (tenkinami reikalavimai ar ne, bei nustatyti defektai).
- 29.3. Paslaugų teikėjas turi pateikti išsamias instrukcijas, kaip teisingai įdiegti Sistemą į testavimo aplinką ir/ar sukonfigūruoti Sistemos tobulinimą/keitimą/vystymą.
- 29.4. Diegimo/išdiegimo instrukcijoje Paslaugų teikėjas privalo:
 - 29.4.1. pateikti diegimo/išdiegimo skriptus,
 - 29.4.2. aprašyti diegimo darbus (žingsnius),
 - 29.4.3. aprašyti kiekvieno žingsnio diegimo preliminarą trukmę,
 - 29.4.4. pateikti rekomendacijas vartotojams naujo funkcionalumo diegimo periodu,
 - 29.4.5. pateikti diegimo į gamybinę aplinką patikros planą.
- 29.5. Kartu su diegimo instrukcija Paslaugų teikėjas turi pateikti atnaujintą naudotojo vadovą, kuriame turi būti pateikta:
 - 29.5.1. įdiegtos funkcijos aprašymas,
 - 29.5.2. veiklos arba automatizuojamos funkcijos schema,
 - 29.5.3. informacija, kokie veiksmai turi būti atlikti prieš pradedant vykdyti funkciją,
 - 29.5.4. informacija, kaip pradėti (pvz., nurodyti meniu kelią) vykdyti automatizuojamą funkciją,
 - 29.5.5. informacija, kaip atlikti (pvz., kokius laukus užpildyti, nurodyti tų laukų paskirtį ir prasmę) automatizuojamą funkciją,
 - 29.5.6. informacija, kokie tolimesni veiksmai turi būti atlikti norint pabaigti funkcijos/užduoties procesą.

- 29.6. Kartu su priėmimo-perdavimo aktu Paslaugų teikėjas įsipareigoja perduoti Klientui detalią dokumentaciją:
- 29.6.1. suderintus pakeitimų analizės protokolus,
 - 29.6.2. pakeitimų techninę specifikaciją,
 - 29.6.3. programų išeities tekstus,
 - 29.6.4. vykdomus kodus,
 - 29.6.5. diegimo instrukcijas,
 - 29.6.6. testavimo rezultatus,
 - 29.6.7. atnaujintą naudotojo vadovą, funkcijų ir duomenų modelių dokumentaciją.
- 29.7. Visą aukščiau nurodytą dokumentaciją Paslaugų teikėjas privalo pateikti lietuvių kalba.
- 29.8. Paslaugų teikėjas turi turėti **dokumentuotas** visas svarbiausias **Sistemos priežiūros funkcijas**:
- 29.8.1. Sistemos administratorių kasdieniai priežiūros darbai (tarnybinių stočių stebėseną (angl. monitoring), atsarginių kopijų darymas, suplanuotų (angl. *scheduled*) užduočių peržiūra ir patikrinimas, pajėgumų planavimas, žurnalinių įrašų peržiūrėjimas, sistemos atnaujinimas ir pan.);
 - 29.8.2. Sistemos kartotinio paleidimo ir atstatymo procedūros, kuriose detalai aprašomi kiekvieno esminio Sistemos komponento atstatymo veiksmai;
 - 29.8.3. prisijungimo prie Sistemos veiksmai;
 - 29.8.4. Sistemos naudotojų vaidmenys (rolės) ir jų galimi atlikti veiksmai Sistemoje;
 - 29.8.5. Sistemos pateikiamų klaidų naudotojams aprašymai bei naudotojų veiksmai gavus klaidos pranešimą;
 - 29.8.6. darbo su Sistema pabaigos veiksmai ir atsijungimo nuo Sistemos procedūra.
- 29.9. Paslaugų teikėjas turi turėti parengtą Kliento Sistemos **atkūrimo planą** (angl. *system recovery plan*), kuriame yra:
- 29.9.1. įvardinti už priežiūrą atsakingi asmenys, apibrėžtas jų vaidmuo ir funkcijos;
 - 29.9.2. identifikuoti ir prioritetizuoti Sistemą palaikantys IT komponentai;
 - 29.9.3. nustatytas priimtinas paslaugų praradimo lygis;
 - 29.9.4. numatyti atitinkamų veiksmų iniciavimo kriterijai;
 - 29.9.5. identifikuotos konkrečios fizinės, personalo, finansų, organizacinės ir techninės priemonės, skirtos veiklos tęstinumui užtikrinti;
 - 29.9.6. detalizuotos procedūros, leidžiančios per numatyta laiko tarpą atkurti ir atstatyti Sistemą, bei ją palaikančius IT komponentus;
 - 29.9.7. numatytos procedūros, taikomos kol bus pilnai atstatyti veiklos procesai (laikinos darbo procedūros);
 - 29.9.8. numatyti komunikavimo veiksmai kritinio gedimo ar nelaimės atveju;
 - 29.9.9. periodinis numatytų veiksmų testavimas, veiklos tęstinumo proceso vertinimas ir gerinimas.
- 29.10. Paslaugų teikėjas turi vykdyti pastovią priežiūrą **sistemų stebėseną**, kad užtikrintų įsipareigojimų (angl. *SLA*) vykdymą

**Priedas Nr. 3 prie Techninės specifikacijos
PASLAUGŲ PRIĖMIMO-PERDAVIMO AKTO FORMA**

**Paslaugų, atliktų pagal sutartį Nr.
perdavimo-priėmimo**

A K T A S Nr.

20____ d
m. _____ .

Šiuo aktu patvirtinama, kad žemiau išvardintos paslaugos yra atliktos ir rezultatai pateikti:

| Nr. | Pavadinimas | Kiekis, (val./vnt.) | Vieneto kaina (€ be PVM) | Suma (€ be PVM) |
|-----------------------|-------------|------------------------|-----------------------------|--------------------|
| 1. | | | | |
| 2. | | | | |
| IŠ VISO: | | | | |
| PVM %: | | | | |
| SUMA SU PVM %: | | | | |

Bendra atliktų paslaugų vertė yra _____ eurai _____ centai įskaitant PVM.

**Priedas Nr. 4 prie Techninės specifikacijos
PASLAUGŲ UŽSAKYMO FORMA**

UŽSAKYMAS NR. [.....]

Vilnius, 2018 m. XX d.

PIRKĖJAS:

[.....]

TIEKĖJAS:

UŽSAKYMO ESMĖ:

Pateikiama užsakomų darbų specifikacija.

REZULTATAS:

Trumpai aprašomas rezultatas.

GARANTIJA:

Atliktiems darbams Vykdytojas įsipareigoja suteikti 3 mėnesių garantinį laikotarpį.

UŽSAKYMO VYKDYMO KONTAKTINIAI ASMENYS:

Vardas Pavardė, Pareigos, tel.: , El. paštas: adresas@adresas.lt;

[.....]

Vardas Pavardė, Pareigos, tel.: , El. paštas: adresas@adresas.lt;

PASLAUGŲ SUTEIKIMO TERMINAS:

Papildomas funkcionalumas bus realizuotas ir įdiegtas per XXX d.d. nuo užsakymo pasirašymo.

Pirkėjas įsipareigoja atliktus darbus ištestuoti per 1 savaitę nuo jų pateikimo datos. Jeigu iki to laiko pastabų Vykdytojui pateikta nebus, tai laikoma, kad klaidų neaptikta ir tuo pagrindu pasirašomas darbų priėmimo-perdavimo aktas ir išrašoma sąskaita-faktūra. Jei užsakymo sudėtyje yra licencijos arba jų naujinimas, Pirkėjas įsipareigoja už jas apmokėti pagal išankstinę sąskaitą, išrašomą užsakymo pasirašymo dieną. Tiekėjas įsipareigoja kokybiškai ir laiku įvykdyti šį užsakymą, Pirkėjas garantuoja apmokėjimą.

PASLAUGŲ KAINA:

| Eil. Nr. | Darbų pavadinimas | Val. |
|-----------|----------------------------------|------|
| 1. | Funkcionalumo pavadinimas | |
| 1.1 | Projektavimas | |
| 1.2 | Programavimas | |
| 1.3 | Testavimas | |
| 1.4 | Dokumentavimas | |
| | Iš viso valandų | |

Priedas Nr. 5 prie Techninės specifikacijos
TIEKĖJO TEIKIAMOS PASLAUGOS

Tiekėjo teikiamos techninio aptarnavimo paslaugos pagal sutartį :

1. **Konsultacijos telefonu.** Pirkėjas turi teisę gauti atsakymą telefonu į klausimus, susijusius su Sistemos ir PĮ veikimu, kurių atsakymai nereikalauja papildomos PĮ duomenų analizės. Jei Tiekėjas negalėjo suteikti tinkamos konsultacijos telefonu iš karto, tai pateikti atsakymus į neatsakytus klausimus Tiekėjas įsipareigoja ne vėliau, kaip per 8 darbo val. po skambučio. Prireikus (esant sudėtingesnei situacijai ir pan.) arba Tiekėjo prašymu Pirkėjas po pokalbio su Tiekėjo atstovu paklausimą laisva forma gali išsiųsti elektroniniu paštu. Esant tokiai situacijai galioja 8 darbo val. laiko terminas.
2. **Konsultacijos elektroniniu paštu ir/arba faksu.** Pirkėjas turi teisę gauti atsakymą elektroniniu paštu ir/arba faksu į bet kokius klausimus, susijusius su Sistemos ir PĮ veikimu. Tokiu atveju Tiekėjas įsipareigoja į Pirkėjo raštu pateikiamus klausimus arba klaidų pranešimus reaguoti ir atsakymą pateikti per 8 darbo val. pranešimo gavimo, jei atsakymai nereikalauja papildomos PĮ duomenų analizės.
3. **PĮ Klaidų ir Kritinių klaidų taisymas.** Tiekėjas identifikuotas Sistemos ir PĮ klaidas taiso 2 savaičių laikotarpyje. Jeigu dėl objektyvių priežasčių Klaidos šalinimui reikalingas ilgesnis laikas, negu Tiekėjo numatyti reakcijos laikai, dėl ilgesnio laiko su Pirkėju susitariama atskirai. Pirkėjas neapmoka darbų, susijusių su Kritinių klaidų ar Klaidų nagrinėjimu, tik tuo atveju, jei Tiekėjas nustato ir abi Šalys sutaria, kad nagrinėjama Klaida/Kritinė klaida yra Programinės įrangos pakeitimų, kuriems galioja garantinis laikotarpis, klaida. Gamintojo klaidų Tiekėjas netaiso.
4. **Parama darbo vietoje.** Po Pirkėjo užsakymo ir paramos teikimo tvarkos susitarimo, Šalių suderintais terminais Tiekėjas suteikia Pirkėjui paramą darbo vietoje.
5. **Sistemos funkcionalumo plėtimas, programavimas.** Paslaugos atliktos pagal Pirkėjo paslaugų užsakymą, sutinkamai su sutartyje nustatytais sąlygomis.
6. **Duomenų tvarkymas.** Jei dėl Pirkėjo kaltės buvo sugadinti duomenys, Tiekėjas juos taiso darbų užsakymo atlikimo sąlygomis.
7. **Užklausos, reikalaujančios analizės.** Tiekėjas privalo įspėti Pirkėją, jeigu jo paslaugoms atlikti reikalingas ilgesnis paslaugų atlikimo terminas, negu nurodyta Užsakyme ir tęsti užklausos nagrinėjimą tik tada, kai jis gauna patvirtinimą iš Pirkėjo, kad pastarasis su tuo sutinka. Tokiu atveju Šalys privalo susiderinti tokios paslaugos atlikimo terminus.