



TECHNINĖ SPECIFIKACIJA

1. SĄVOKOS IR SUTRUMPINIMAI

- 1.1. **Pirkėjas** – AB „KN Energies“.
- 1.2. **Tiekėjas** – ūkio subjektas – fizinis asmuo, privatusis juridinis asmuo, viešasis juridinis asmuo, kitos organizacijos ir jų padaliniai ar tokių asmenų grupė, su kuriuo Pirkėjas sudaro Sutartį.
- 1.3. **Sutartis** – Sutartis, sudaroma tarp Tiekėjo ir Pirkėjo dėl Pirkimo objekto.
- 1.4. **Pirkimo objektas** – Paslaugos.
- 1.5. **Paslaugos** – IT veiklos testinimą užtikrinančio rezervinio duomenų centro, ryšio su juo, ugniasienės ir DR plano testavimo ir dokumentavimo paslaugos (toliau – Paslaugos).

2. PIRKIMO OBJEKTAS

- 2.1. IT sistemų veiklos testinimo užtikrinimo paslaugos (toliau – Pirkimo objektas).
- 2.2. IT veiklos testinimą užtikrinančio rezervinio duomenų centro, ryšio su juo, ugniasienės ir DR plano testavimo ir dokumentavimo paslaugos susideda iš:
 - 2.2.1. IS avarinio perkėlimo ir atstatymo (toliau – DR) rezerviniame duomenų centre (DRaaS) paslaugų;
 - 2.2.2. Ugniasienės FWaaS paslaugų;
 - 2.2.3. Duomenų perdavimo tinklo paslaugų;
 - 2.2.4. Atstatymo po avarijos plano (toliau - DRP) paruošimo ir jo testavimo paslaugų.
- 2.3. Pirkimo objektas į dalis neskaidomas.

3. ESAMA SITUACIJA

- 3.1. Šiuo metu didžioji dalis Pirkėjo vidinių sistemų (toliau – IS) veikia nuosavoje IT infrastruktūroje, sudarytoje iš tarnybinių stočių techninės įrangos.
- 3.2. Naudojama tarnybinių stočių techninė įranga nėra plečiama. Esama techninė įranga naudoja VMware virtualizavimo technologiją.
- 3.3. Kritinės IS – Pirkėjo virtualūs serveriai (toliau – VM): Domeno kontrolieris (1 vnt.), Finansinė apskaita (3 vnt.), Dokumentų valdymo sistema (1 vnt.), Krovos ir užsakymų valdymo (9 vnt.), Duomenų bazių serveris (1 vnt.), Spausdinimo valdymo sistema (1 vnt.), kitos paskirties (3 vnt.) – iš viso 19 vnt., **Oracle DB serveris – 1 vnt.**
 - 3.3.1. Naudojamos operacinės sistemos - Microsoft Windows, Linux:
 - 1.1. Windows Server 2016/8/20
 - 3.3.1.1. Windows Server 2019
 - 3.3.1.2. Windows Server 2022
 - 3.3.1.3. Debian Linux
 - 3.3.2. Kritinių IS virtualių serverių minimalūs resursai (kiekis):
 - 3.3.2.1. vCPU – 98 vnt.
 - 3.3.2.2. RAM – 284 GB
 - 3.3.2.3. SSD – 7 TB
 - 3.3.3. Naudojamų potinkių minimalus kiekis – 5
 - 3.3.4. VPN naudotojų minimalus kiekis – 300
 - 3.3.5. Naudojamų išorinių IP adresų kiekis – 10
- 3.4. Esamas Pirkėjo WAN tinklo sprendimas, realizuotas MPLS VPN technologijos pagrindu, apjungia 5 vienas nuo kito nutolusius padalinius.

4. PIRKIMO OBJEKTO APRAŠYMAS

- 4.1. Pirkėjas, siekdamas užtikrinti aukštą kritinių informacinių sistemų patikimumą ir veiklos testinimą bei lankstumą, planuoja įsigyti Paslaugas.

- 4.2. Paslaugos apima Pirkėjo kritinėms IS veikti reikalingų virtualių resursų rezervavimą ir, įvykus nelaimei nuosavoje Pirkėjo infrastruktūroje ir aktyvavus avarinį perkėlimą, jų dubliavimą, duomenų perdavimo tinklo, Interneto ryšio paslaugą ir ugniasienės paslaugą Tiekėjo duomenų centre.
- 4.3. Paslaugos apima Pirkėjo esamo WAN tinklo infrastruktūros sujungimą su rezervinio duomenų centro infrastruktūra.
- 4.4. Paslaugos yra visiškai integruotos į esamą Pirkėjo WAN tinklo architektūrą.
- 4.5. Paslaugos kartu yra pasiekiamos ir iš nutolusių mobiliųjų darbo vietų, per tuo tikslu Rezerviniame duomenų centre veikiantį VPN šliuzą.
- 4.6. Aktyvavus avarinį perkėlimą, Paslaugos perima ir vykdo centrinio padalinio pagrindinio duomenų centro ir maršrutizatoriaus rolę bei teikia Interneto ryšį, tarpusavio duomenų apsikeitimo paslaugą Pirkėjo padaliniams bei užtikrina integracijas su trečiosiomis šalimis.
- 4.7. Paslaugos yra teikiamos 24 (dvidešimt keturias) valandas per parą ir 7 (septynias) dienas per savaitę, nuo Paslaugų užsakymo ir parengimo darbui datos. Paslaugos visą jų teikimo laikotarpį turi apimti visą joms teikti reikalingą techninę, programinę įrangą, apimant jos įsigijimą, įdiegimą bei priežiūrą, šios įrangos veikimui reikalingos infrastruktūros užtikrinimą, visas jai teikti reikalingas elektros energijos sąnaudas bei kitas su Paslaugų teikimu susijusias sąnaudas.
- 4.8. Paslaugos apima Pirkėjo konsultavimą įsigytų Paslaugų teikimo ir jų funkcijų klausimais pagal Pirkėjo poreikius. Konsultacijų kaina turi būti įskaičiuota į Paslaugų kainą.

5. REIKALAVIMAI PIRKIMO OBJEKTUI

IT SISTEMŲ VEIKLOS TĘSTINUMO UŽTIKRINIMO PASLAUGOS	
Pirkimo objektui taikomas žaliasis kriterijus	
5.1.	Perkamos nematerialaus pobūdžio paslaugos, nesusijusios su materialaus objekto sukūrimu, kurių teikimo metu nėra numatomas reikšmingas neigiamas poveikis aplinkai, nesukuriamas taršos šaltinis ir negeneruojamos atliekos. Pirkėjas siekia, jog jo ir Tiekėjo veiksmai darytų kuo mažesnę poveikį aplinkai, todėl: - Viešojo pirkimo ir sutarties vykdymo metu bendravimas tarp Tiekėjo ir Pirkėjo bus vykdomas tik elektroninėmis priemonėmis (CVP IS priemonėmis, telefonu, elektroniniu paštu, ar kt.); - Visa dokumentacija, susijusi su Sutarties vykdymu teikiama Pirkėjui ir Tiekėjui elektroninėmis priemonėmis (CVP IS priemonėmis, elektroniniu paštu ar kt.); - Sutartį bus siekiama pasirašyti tik elektroninėmis priemonėmis (elektroniniu parašu); - Tiekėjas įsipareigoja mažinti popieriaus sunaudojimą, atsisakyti nebūtino dokumentų kopijavimo ir spausdinimo, jeigu bus naudojamos kanceliarinės priemonės, jos turi būti pagamintos iš perdirbtų žaliavų arba tinkamos perdirbimui; - Esant būtinybei spausdinti, Tiekėjas įsipareigoja naudoti perdirbtą popierių, kuris atitinka žaliojo pirkimo reikalavimus, patvirtintus Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 „Dėl Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo patvirtinimo“ (toliau – Aprašas); - Tiekėjas įsipareigoja Paslaugų teikimo metu susidariusias atliekas rūšiuoti ir atliekas tinkamas perdirbimui ar pakartotinam panaudojimui perduoti tokias atliekas turinčiam teisę tvarkyti atliekų tvarkytojui, o netinkamas perdirbimui ar pakartotinam panaudojimui - utilizuoti specialiai tam skirtose vietose. - Jei Paslaugų vykdymo metu Tiekėjo naudojamos prekės/medžiagos/žaliavos turi būti tiekiamos ar perduodamos antrinėje pakuotėje, jos turi atitikti pakuotėms nustatytus minimalius aplinkos apsaugos kriterijus, nebent tai prieštarauja higienos normoms: pakuotės turi būti laikytinos perdirbamosiomis pakuotėmis pagal Lietuvos Respublikos mokesčio už aplinkos teršimą įstatymo nuostatas. - Tiekėjas įsipareigoja siekti, kad Tiekėjo specialistai, teikiantys paslaugas, atvykimui į paslaugų vykdymo vietą rinktųsi netaršias transporto priemones, kurios atitinka žaliojo pirkimo reikalavimus, patvirtintus Apraše; - Tiekėjas įsipareigoja siekti, kad būtų pasirenkamas optimalus maršrutas Tiekėjo specialistų atvykimui į paslaugų vykdymo vietą; - Tiekėjas įsipareigoja siekti, kad paslaugoms teikti būtų pasiūlytas arčiausiai numatomos paslaugų vykdymo vietos esantis specialistas;

	- Tiekėjas įsipareigoja siekti, kad jo veiksmai neterštų aplinkos ir nekeltų pavojaus sveikatai ir taip būtų laikomasi Aprašo 4.4.4 punkte nustatyto aplinkosauginio principo.	
Reikalavimai dėl atitikties nacionalinio saugumo interesams		
5.2.	5.2.1. Tiekėjo siūlomos paslaugos turi nekelti grėsmės nacionaliniam saugumui. Laikoma, kad tiekėjo siūlomos paslaugos kelia grėsmę nacionaliniam saugumui, kai: 1) paslaugų teikimas būtų vykdomas iš VPĮ 92 straipsnio 14 dalyje numatyto sąraše nurodytų valstybių ar teritorijų. 5.2.1.1. Jei pagal vertinimo rezultatus Pasiūlymas galės būti pripažintas Laimėjusiu (iki Pasiūlymų eilės nustatymo), tikrinant pasiūlymo atitiktį VPĮ 37 str. 9 d./ PĮ 50 str. 9 d. reikalavimams, Perkančiajam subjektui pareikalavus, tiekėjas turės pateikti vieną ar kelis šiuos dokumentus: 1) juridinio asmens vadovo patvirtintą juridinio asmens steigimo dokumentų kopiją, 2) Juridinių asmenų registro išplėstinį išrašą su istorija, 3) Juridinių asmenų dalyvių informacinės sistemos išrašą, 4) asmens tapatybę patvirtinančio dokumento (tapatybės kortelės ar paso) kopiją, 5) leidimo verstis atitinkama ūkine veikla patvirtinančio dokumento (pavyzdžiui, verslo liudijimo, individualios veiklos pažymėjimo ir pan.) kopiją, 6) pažymą apie deklaruotą gyvenamąją vietą arba atitinkamus valstybės narės ar trečiosios šalies dokumentus, 7) kitus perkančiajam subjektui priimtinus dokumentus. Dokumentai, kuriuose nenurodytas galiojimo terminas, turi būti išduoti ar atspausdinti iš informacinės sistemos ne anksčiau kaip prieš 3 mėnesius iki tos dienos, kurią perkančiojo subjekto prašymu tiekėjas turi pateikti dokumentus. 5.2.2. Tiekėjo siūlomos prekės (įskaitant jų gamintojus), paslaugos ar darbai turi nekelti grėsmės nacionaliniam saugumui. Laikoma, kad tiekėjo siūlomos prekės (įskaitant jų gamintojus), paslaugos ar darbai kelia grėsmę nacionaliniam saugumui, kai Lietuvos Respublikos Vyriausybė yra priėmusi sprendimą, patvirtinantį, kad ketinamas sudaryti ar sudarytas sandoris neatitinka nacionalinio saugumo interesų vadovaujantis Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymu. Pirkimo metu atliekant patikrą dėl atitikties nacionalinio saugumo interesams, Tiekėjas turės pateikti tokiai patikrai atlikti reikalingus dokumentus. 5.2.3. Tiekėjo pasiūlymas bus atmestas, jeigu yra bent viena iš nurodytų sąlygų (PĮ 58 str. 41).	
Reikalavimai IT veiklos tęstinumą užtikrinančio rezervinio duomenų centro, ryšio su juo, ugniasienės ir DR plano dokumentavimo ir testavimo paslaugoms		
Eil. Nr.	Reikalavimas	Reikalavimo išpildymas
5.3.	Tiekėjas turi pateikti IS avarinio perkėlimo ir atstatymo rezerviniame duomenų centre paslaugas.	5.3.1. Tiekėjas turi užtikrinti Pirkėjo kritinių IS avarinį perkėlimą į Tiekėjo duomenų centrą: 5.3.1.1. Tiekėjas savo pastangomis privalo atlikti visus avariniam perkėlimui būtinus debesų kompiuterijos techninės platformos Tiekėjo duomenų centre konfigūravimo darbus ir užtikrinti interneto bei duomenų perdavimo tinklo ryšį tarp debesų kompiuterijos paslaugos Tiekėjo duomenų centro ir Pirkėjo. 5.3.1.2. Tiekėjas turi pateikti visas reikiamas programines priemones ir licencijas, reikalingas rezerviniam kopijavimui į Tiekėjo duomenų centrą ir duomenų atstatymui iš Tiekėjo duomenų centro į Pirkėjo duomenų centrą. 5.3.1.3. Kritinių IS rezervinis kopijavimas turi būti vykdomas: - virtualių mašinų lygyje ne rečiau kaip du kartus per parą; - Duomenų bazių – su pirkėju suderintu dažnumu ir būdu, ne dažniau kaip 4 kartus per parą.

		5.3.1.4. Rezervinės kopijos turi būti saugomos ne mažiau kaip septynias dienas. 5.3.1.5. Rezerviniam kopijavimui turi būti naudojama Veeam platforma. 5.3.1.6. Tiekėjas į savo duomenų centrą turi perkelti Pirkėjo pateiktus fizinės infrastruktūros duomenis ir nustatymų rinkmenas. 5.3.1.7. Tiekėjas savo duomenų centre turi aktyvuoti Pirkėjo kritinių IS virtualias mašinas po avarinio perkėlimo ir užtikrinti IS veikimą bei pasiekiamumą. 5.3.2. Tiekėjas turi užtikrinti visas technines, programines priemones, sąnaudas (pvz. resursai, licencijos, elektra ir t.t.) perkelti Pirkėjo IS duomenis į rezervinio duomenų centro platformą. 5.3.3. Pirkėjo kritinių IS avarinis perkėlimas į Tiekėjo duomenų centrą turi būti vykdomas minimaliai trikdančią organizacijos darbą. Avariniam perkėlimui reikalingi papildomi įrankiai ir resursai turi būti suteikti neatlygintinai. 5.3.4. Tiekėjas turi pateikti programinės įrangos diegimo paketą ir paruoštus importuoti nuostatų rinkinius Pirkėjui, reikalingus atlikti pradinį VPN klientų diegimą Pirkėjo nutolusiose darbo vietose bei pakartotinius diegimus pagal Pirkėjo užklausas. 5.3.5. Avarinio perkėlimo aktyvavimo laikotarpiu gali būti naudojami arba tie patys, kurie veikia Pirkėjo tinkle, arba Tiekėjo suteikti išoriniai IP adresai. Aktyvavus avarinį perkėlimą, Tiekėjas turi užtikrinti, kad per trumpiausią laiką Pirkėjo atitinkamų iš išorės naudojamų resursų DNS vardai būtų nukreipti į šiuos IP adresus. 5.3.6. Avarinio perkėlimo aktyvavimo principas turi būti paremtas VM/paslaugų įjungimo/išjungimo principu, t. y. nereikalausti programinės įrangos keitimo, perinstaliavimo. 5.3.7. Atlikus avarinį perkėlimą į rezervinį duomenų centrą ir aktyvavus Pirkėjo IS virtualias mašinas, turi būti užtikrintas nenutrūkstamas IS ryšys su kitomis Pirkėjo sistemomis ir trečiosiomis šalimis. 5.3.8. Visos avarinio perkėlimo sąnaudos ir kiti susiję kaštai turi būti įtraukti į pasiūlymo kainą. 5.3.9. Įvykus avarinei situacijai Pirkėjo duomenų centre, maksimali leidžiama IS prastova iki IS atstatymo rezerviniame duomenų centre negali viršyti 24 val. 5.3.10. IS avarinio perkėlimo paslaugos parengties lygis turi atitikti paslaugų pateikimo lygį 24x7. 5.3.11. Maksimalus toleruojamas IS duomenų / nustatymų praradimo intervalas nuo avarinės situacijos susidarymo momento negali viršyti 12 val. 5.3.12. Tiekėjas turi užtikrinti DR aplinką, tinkamą Oracle Standard Edition 2 duomenų bazei (iki 2 CPU), pilnai atitinkančią Oracle licencijavimo ir techninius reikalavimus, įskaitant: 5.3.12.1. CPU ribojimą iki licencijuojamos apimties 5.3.12.2. suderinamumą su Oracle DB veikimu virtualioje aplinkoje; 5.3.12.3. galimybę atlikti DB lygio atstatymą; 5.3.12.4. suderinamumą su Oracle backup mechanizmais (RMAN ar analogiškais)
5.4.	Tiekėjo duomenų centras turi atitikti šiuos reikalavimus.	5.4.1. Siekiant užtikrinti Pirkėjo IS pasiekiamumą ir veiklos tęstinumą aktyvavus avarinį atstatymą po nelaimės, turi būti galima 2 (ar daugiau) duomenų centrų resursus naudoti lygiagrečiai (vienu

	Turi būti pateikti pagrindžiantys dokumentai	metu), t.y. tarp duomenų centrų turi veikti sinchroninė duomenų replikacija duomenų saugyklų lygyje. 5.4.2. Duomenų centrai turi būti įrengti Lietuvos Respublikos teritorijoje (pasiūlyme nurodyti tikslūs duomenų centrų adresus). Atstumas tarp duomenų centrų turi būti ne mažesnis nei 8 kilometrai matuojant tiesia linija. Duomenų centrų ir juose esančios techninės įrangos (tarnybinių stočių, duomenų masyvų, nepertraukiamo maitinimo šaltinių, oro kondicionavimo įrenginių, dujų gesinimo sistemų) nuosavybės teisės turi priklausyti Tiekėjui. 5.4.3. Duomenų centrai neturi būti įrengti požeminiame ar paskutiniame pastato aukšte arba patalpose, kuriose arba virš kurių yra vandentiekio, kanalizacijos, šildymo sistemos vamzdinių ar aušinimo sistemos vamzdinių. 5.4.4. Paslaugos teikimui naudojama techninė įranga turi būti išdėstyta ne mažiau kaip dviejuose duomenų centruose, vienas iš jų turi būti ne mažesnis kaip „Tier-III“ patikimumo, t.y. turėti „Tier III Design“ ir „Tier III Facility“ arba lygiavertčius sertifikatus. 5.4.5. Duomenų centro kompiuterinės įrangos našumo ir pajėgumo parametrai turi būti ne prastesni nei: 5.4.5.1. Ne mažiau nei 4 (keturios) fizinės tarnybinės stotys, skirtos tarnybinių stočių virtualizavimo platformai. Jos turi būti apjungtos į aukšto patikimumo blokinį (angl. cluster), kiekviename iš duomenų centrų talpinant ne mažiau kaip po 2 fizinės tarnybinės stoties iš aukšto patikimumo blokino. 5.4.5.2. Fizinių tarnybinių stočių, skirtų tarnybinių stočių virtualizavimo platformai, procesorių našumas 2 (dvejų) procesorių aparatinėje platformoje ne mažiau nei: 5.4.5.2.1. SPEC2017_int_speed_base = 11 5.4.5.2.2. SPEC2017_fp_speed_base = 134 5.4.5.2.3. SPEC2017_int_rate_base = 257 5.4.5.2.4. SPEC2017_fp_rate_base = 227 <i>Pastaba: Našumo rezultatai turi būti išmatuoti su siūlomu procesoriumi bet kurioje aparatinėje platformoje. Našumo testų rezultatai turi būti viešai publikuoti www.spec.org puslapyje. Pasiūlyme būtina nurodyti fizinių tarnybinių stočių, kurios bus skiriamos tarnybinių stočių virtualizavimo platformai, procesorių skaičių, gamintoją ir modelį, dažnį, veikiančių branduolių skaičių, spartinančiosios atminties dydį, sisteminės magistralės dažnį.</i> 5.4.5.3. Suminis fizinių tarnybinių stočių operatyvinės atminties kiekis (RAM) ne mažesnis nei 6000 GB. 5.4.5.4. Fizinių tarnybinių stočių, skirtų tarnybinių stočių virtualizavimo platformai, resursų (CPU ir RAM) naudojimas neturi viršyti 70%. 5.4.5.5. Duomenų saugyklų našumo parametrai. 5.4.5.6. Visi komponentai dubliuojami, įskaitant: 5.4.5.6.1. Ne mažiau kaip du valdymo moduliai; 5.4.5.6.2. Ne mažiau kaip du maitinimo šaltiniai. 5.4.5.7. Duomenų vientisumui neturi turėti įtakos pavieniai duomenų saugyklos kietųjų diskų gedimai.
--	--	--

		5.4.5.8. Duomenų saugykla su fizinėmis tarnybinėmis stotimis turi būti sujungta neblogesne nei iSCSI arba FC sąsaja, kurios greitis ne mažiau kaip 16 Gbps.
5.5.	Tiekėjo DR sprendimo duomenų perdavimo tinklas turi atitikti šiuos reikalavimus	5.5.1. Tiekėjas turi pasiūlyti sprendimą, kuris būtų integruotas į Pirkėjo veikiantį WAN duomenų perdavimo tinklą, kuriuo Pirkėjo Duomenų Centras ir Padaliniai sujungti į bendrą tinklą IP protokolu, arba apimtų visus padalinius nauju, ne prastesnių parametrų negu eksploatuojamas Pirkėjo, WAN duomenų perdavimo tinklu. Reikalaujama, kad Tiekėjas pasiūlytų tokį sprendimą, kuris būtų standartizuotas ir veiktų remiantis atvirais protokolais. 5.5.2. Tiekėjas privalo užtikrinti nepertraukiamą perėjimą iš šiuo metu eksploatuojamo duomenų perdavimo tinklo į išplėstą arba naują. 5.5.3. Siūlomas duomenų perdavimo tinklo sprendimas turi būti suprojektuotas ir įrengtas laikantis hierarchinės struktūros ir turi atitikti rekomendacijas dėl OSI ir TCP/IP standartinių modelių. 5.5.4. Tinklo sprendimo įgyvendinimui turi būti naudojama BGP/MPLS VPN technologija (žr. IETF komiteto dokumentą RFC 2547, TIA ir IETF standartus bei rekomendacijas, pateikiamas http://www.ietf.org/html.charters/mpls-charter.html), kuri yra pageidaujama pagrindinio Tiekėjo tinklo, kurio paslaugas Pirkėjas ketina įsigyti, technologija. 5.5.5. Tiekėjas gali siūlyti ir kitomis technologijomis (ne vien MPLS VPN) pagrįstą Pirkėjo duomenų perdavimo tinklo sprendimą. 5.5.6. Tiekėjas turi pateikti detalią informaciją, nurodant, kuri siūlomo duomenų perdavimo tinklo dalis (infrastruktūra) yra Tiekėjo nuosavybė. Jeigu Tiekėjas ketina remtis subteikėjų ar kitų ūkio subjektų infrastruktūra, kartu su pasiūlymu privalo nurodyti, kuri (-ios) tinklo dalis (-ys) priklauso subteikėjams ar kitiems ūkio subjektams, įvardinant tinklo atkarpas ir jų savininkus. 5.5.7. Siekiant užtikrinti stabilią ir prognozuojamą paslaugų kokybę, stuburinis perdavimo tinklas neturi būti priklausomas nuo įvairių išorinių faktorių, pvz., drėgmės, temperatūros, kritulių ir pan. Pageidautina naudoti požemines perdavimo linijas, ne elektrinius, bet optinius pluoštinius kabelius. 5.5.8. Jei reikalinga, Tiekėjas Pirkėjui duomenų perdavimo paslaugas teikia naudodamas savo ar nuomojamą įrangą. Jeigu Tiekėjas ryšio linijas nuomojasi, jis turi pateikti ryšio linijų savininko dokumentą, o tais atvejais, kai Paslaugos teikiamos per bendro naudojimo atsietų varinių arba optinių kabelių prieigų resursus, kurių naudojimas reglamentuojamas Ryšių reguliavimo tarnybos teisinais aktais, įpareigojančiais teikti tokias paslaugas didelę įtaką rinkoje turinčius operatorius visiems pageidaujantiems vienodomis viešai paskelbtomis sąlygomis, nuorodą į konkrečius teisinių aktų punktus, tuo įrodydamas, kad bus tenkinami Paslaugų lygmens susitarime (SLA) nurodyti reikalavimai visam Sutarties galiojimo laikui. 5.5.9. Ryšys tarp Tiekėjo DC ir esamo (kiekvieno) WAN tinklo taško turi būti realizuojamas dviem nepriklausomomis fizinėmis ryšio linijomis ir turi turėti du Tiekėjo galinės įrangos komplektus. Viena iš šių ryšio linijų yra skirta rezervinio ryšio užtikrinimui. Ryšys su Pirkėjo (arba WAN ryšio paslaugos Tiekėjo) įranga turi

		būti palaikomas per Full Duplex 1000Base TX Ethernet sąsają su IEEE 802.1Q paketavimu (encapsulation). 5.5.10. Jei fizinė ryšio linijų sparta didesnė už pralaidumą ir Tiekėjas savo tinkle įdiegia spartos ribojimo technologiją, tada Tiekėjo galinė įranga turi būti pajėgi formuoti srautų klases ir (arba) riboti spartą. Būtina užtikrinti, kad aukštesnio prioriteto srautas iš vartotojo (kliento) įrangos per Tiekėjo tinklą būtų išsiunčiamas pirmiausia, o Tiekėjo tinklas jo neatmestų arba nepriskirtų žemesnei klasei dėl viršytos spartos. 5.5.11. Tiekėjui neleidžiama pernuomoti garantuojamo pralaidumo papildomiems abonentams. 5.5.12. Visa tinklo galinė įranga turi būti stebima ir valdoma nuotoliniu būdu. 5.5.13. Tiekėjas turi sudaryti galimybę naudotis rezerviniu tinklu neribojant persiunčiamų duomenų kiekio. 5.5.14. Pagrindiniai ir rezerviniai tinklai turi veikti pastoviai, naudojimas rezerviniu tinklu negali būti ribojamas. 5.5.15. Tiekėjas turi turėti galimybę prijungimo taškų ryšių pralaidumus padidinti per 5 (penkias) darbo dienas iki 200% pradinės reikšmės be atnaujinimo išlaidų. 5.5.16. Taškuose tarp Tiekėjo įrangos ir Pirkėjo tinklo (ar WAN ryšio Tiekėjo) turi būti palaikomas statinis maršrutizavimas ir atvirųjų standartų maršrutizavimo protokolai RIPv2, OSPF, BGP. Tiekėjo įranga turės skelbti likusios Tiekėjo tinklo dalies gaunamą maršrutizavimo informaciją per dinaminį maršrutizavimo protokolą. 5.5.17. Bendras paslaugos pateikiamumas turi būti ne mažesnis nei 99.7%. 5.5.18. Ryšiui Tiekėjo tinklas turi būti pajėgus aptarnauti mažiausiai 5 srautų klases: realiojo laiko srautų balso ir vaizdo klasė, dvi spartai, vėlinimui ir (arba) paketų praradimui jautrių srautų klases ir „mažiausios blogybės“ (best effort) klasę. Be to, turi būti rezervuojamas pralaidumas valdymo srautui, pvz., maršrutizavimo protokolų atnaujinimams, kurie apdorojami atskirai. 5.5.19. Siūlomas duomenų perdavimo tinklo sprendimas neturi sumažinti arba panaikinti Pirkėjo WAN tinklo apsaugos nuo trečiųjų šalių antpuolių, žlugdančių tinklo darbą (Denial of Service). 5.5.20. Tiekėjas turi turėti aptarnavimo centrus Klaipėdoje ir Vilniuje, galinčius atlikti patikimumo užtikrinimo ir gedimų šalinimo funkcijas. 5.5.21. Tiekėjas turi pateikti įrengimo schemas ir aprašymus, iš kurių būtų matyti, kaip tenkinami išvardyti patikimumo reikalavimai. Skaičiavimai turi būti atliekami standartiniu telekomunikacijų pramonės metodu MTBF nustatyti. Tai Telcordia (anksčiau Bellcore) metodas Parts Count Method, aprašytas Bellcore TR-332 (http://telecom-info.telcordia.com/site-cgi/ido/index.html). Skaičiuojant patikimumą turi būti atsižvelgiama į nurodytą vidutinę darbingumo atkūrimo trukmę (MTTR). 5.5.22. Galimybė fiziškai pasiekti įrenginius, kuriuose palaikomos Tiekėjo ir Pirkėjo maršrutizavimo lentelės (pvz., PE ir P maršrutizatoriai MPLS VPN tinkluose), turi būti stebima ir
--	--	--

		ribojama. Tokių įrenginių laikymas Tiekėjo patalpose leistinas tik esant specialiam susitarimui dėl saugos. 5.5.23. Maršrutizavimo lentelių sauga. Dinaminio maršrutizavimo protokolų atnaujinimai turi būti filtruojami norint apsisaugoti nuo paketų – apsimetėlių. Maršrutizatorių maršrutizavimo protokolų susiejimo operacijos metu turi būti nustatomas šalių tapatumas. 5.5.24. Tiekėjas turi garantuoti, kad Pirkėjui skirti Tiekėjo maršrutizatoriai ir ryšio linijos nebus naudojamos bendrai su kitomis įmonėmis ir (arba) su kitais klientais. 5.5.25. VPN srautai turi būti atskirti ir tarpusavyje, ir nuo kitų Tiekėjo srautų, Tiekėjo tinkle turi būti užtikrinami aukšti duomenų saugos lygiai. Iš VPN tinklo į Tiekėjo tinklo galinės įrangos maršrutizavimo lentelę stebėjimo tikslu, leidžiama pateikti tik vieno sąsajos adreso maršrutui. Toks maršruto perdavimas turi padėti išvengti prijungimo taškų tarpusavio bendravimo. Kreipimosi teisių sąrašai ir ugniasienės turi apsaugoti valdymo sąsają ir atidaryti tik būtinus prievadus. 5.5.26. Ugniasienė: Sprendime naudojama ugniasienė turi būti realizuota kaip virtualus įrenginys (angl. Virtual Appliance) arba užtikrinama kaip paslauga Tiekėjo infrastruktūros pusėje. Tiekėjas turi aiškiai įvardinti siūlomos ugniasienės gamintoją, modelį (jei taikoma) arba virtualios platformos specifikacijas. 5.5.27. Tiekėjo įranga turi užtikrinti sąsajas su Pirkėjo LAN įranga. 5.5.28. Ryšio taškų terminavimui Tiekėjas privalo pateikti savo parinktą maršrutizatorių, užtikrinantį pilną DRaaS paslaugos funkcionalumą ir suderinamumą. Srauto apsaugai užtikrinti Tiekėjas privalo pateikti virtualią ugniasienę arba realizuoti ugniasienės sprendimą savo infrastruktūros pusėje. 5.5.29. Konkursą laimėjęs Tiekėjas ir Pirkėjas turi sudaryti ir pasirašyti aptarnavimo lygio susitarimą (SLA), kuriame būtų užfiksuoti duomenų perdavimo tinklo Sutarties šalių vykdymo priežiūros reikalavimai ir procedūros. Aptarnavimo lygio susitarimas yra teisinis dokumentas – pagrindinė duomenų perdavimo tinklo Sutarties dalis arba priedas. Aptarnavimo lygio susitarime (SLA) išvardijamos tinklo priežiūros sąlygos, reikalingos Pirkėjui nepertraukiamo tinklo veiklai palaikyti. Be to, aptarnavimo lygio susitarime turi būti nurodytos aptarnavimo lygio specifikacijos, aiškiai apibūdinančios efektyvumo lygį ir rezultatus, kurių Pirkėjas tikisi iš Tiekėjo. Šiuos efektyvumo standartus Tiekėjas privalo tenkinti arba viršyti. Tiekėjas pasiūlyme turi pateikti prisijungimo duomenis prie savo siūlomos stebėjimo sistemos. 5.5.30. WAN dalys (CPE, ryšio linijos ir pagrindinis tinklas) turi būti valdomos iš vieno Tiekėjo tinklo operacinio centro (NOC). 5.5.31. Tiekėjo tinklo valdymo sistema turės palaikyti Tinklo parametrų stebėjimą ir kaupti informaciją, reikalingą sudaryti ataskaitoms, kurios pagal SLA (service-level agreement) turi būti pateikiamos Pirkėjui. 5.5.32. Tiekėjas įsipareigoja per pirmą tinklo paslaugų teikimo mėnesį pademonstruoti, kaip Tinklo stebėjimo (monitoringo) sistema veikia įprastinėmis darbo sąlygomis ir įvykus gedimui. 5.5.33. Tiekėjo Tinklas turi būti įrengtas laikantis SNMP protokolo palaikymo reikalavimų visų kritinių Tinklo įrenginių stebėjimo (monitoringo) tikslu.
--	--	---

		5.5.34. Pirkėjui turi būti suteikta galimybė stebėti kanalų kokybinius bei SLA parametrus, suteikiant ir galimybę stebėti galinės Tiekėjo perdavimo įrangos (maršrutizatorių) parametrus skaitymo (read only) režime.
5.6.	Ugniasienės paslaugoms Tiekėjo duomenų centre taikomi reikalavimai	5.6.1. Ugniasienės paslaugos turi būti teikiamos iš Tiekėjo duomenų centro ir turi būti pilnai suderintos su resursų nuomos ir DR paslaugomis. 5.6.2. Paslaugų teikimo laikas - 24 valandos per parą ir 7 dienos per savaitę. 5.6.3. Paslaugų pasiekiamumas - ne blogiau kaip 99,95% per mėnesį. 5.6.4. DR paslaugoms esant neaktyvioms, Ugniasienė turi būti sukonfigūruota blokuoti visą įeinantį ir išeinantį, išskyrus su dubliuojamos infrastruktūros duomenų apsikeitimo funkcionalumu ir administravimu susijusį, duomenų srautą. 5.6.5. DR paslaugoms esant aktyvioms, Ugniasienė turi būti sukonfigūruota užtikrinti saugų įeinantį ir išeinantį Interneto ir su dubliuojamos infrastruktūros duomenų apsikeitimo funkcionalumu ir administravimu susijusį duomenų srautą visiems Pirkėjo „baltajame sąrašė“ esantiems potinkiems, blokuoti visą įeinantį ir išeinantį Interneto duomenų srautą potinkiems, nesantiems „baltajame sąrašė“. 5.6.6. Turi būti užtikrintos šios (apimant bet neapsiribojant) ugniasienės savybės: 5.6.6.1. Našumas: 5.6.6.1.1. Ugniasienės greیتaveika – ne mažiau 15 Gbps; 5.6.6.1.2. Lygiagrečių sesijų kiekis – ne mažiau nei 2.6 mln. vnt.; 5.6.6.1.3. Naujų sesijų per sekundę kiekis – ne mažiau nei 100 tūkst. vnt.; 5.6.6.1.4. IPSec VPN palaikoma greیتaveika – ne mažiau 1.5 Gbps; 5.6.6.1.5. SSL-VPN palaikoma greیتaveika – ne mažiau 830 Mbps; 5.6.6.1.6. Įsilaužimų prevencijos (IPS) greیتaveika – ne mažiau 5.5 Gbps. 5.6.6.2. Bendro pobūdžio ugniasienės funkcijos: 5.6.6.2.1. Veiklos tipas – NAT, PAT, Transparent (Bridge); 5.6.6.2.2. „Policy-Based NAT“ funkcionalumas; 5.6.6.2.3. „VLAN Tagging (802.1Q)“ funkcionalumas arba lygiavertis standartas. 5.6.6.3. Įrenginio VPN funkcijos ir našumas: 5.6.6.3.1. IPSec, SSL-VPN dedikuotų tunelių palaikymas; 5.6.6.3.2. 3DES, AES256 arba lygiavertčius šifravimo algoritmus; 5.6.6.3.3. „Dead Peer Detection“ funkcionalumas; 5.6.6.3.4. „IPSec NAT Traversal“ funkcionalumas; 5.6.6.3.5. SHA-1, SHA-256, SHA-512, MD5 autentifikacijos palaikymas; 5.6.6.3.6. Palaikomų IPSec VPN tunelių kiekis - ne mažiau 100 vnt.; 5.6.6.3.7. Palaikomų VPN tunelių kiekis (SSL-VPN) – ne mažiau 200 vnt. 5.6.6.4. IPS funkcijos: 5.6.6.4.1. Darbas IPS režime; 5.6.6.4.2. Darbas IDS režime; 5.6.6.4.3. Protokolų anomalijų palaikymas; 5.6.6.4.4. Modifikuotų taisyklių rinkinių (angl. signature) palaikymas; 5.6.6.4.5. Automatinis įsilaužimų duomenų bazės atnaujinimas; 5.6.6.4.6. IPv6 palaikymas. 5.6.6.5. Srautų valdymas: 5.6.6.5.1. Duomenų srauto ribojimas pagal ugniasienės taisykles; 5.6.6.5.2. Duomenų srauto ribojimas pagal IP adresą; 5.6.6.5.3. Duomenų srauto ribojimas pagal aplikaciją;

	5.6.6.5.4. Diferencijuotų servisų palaikymas (angl. DiffServ); 5.6.6.5.5. Garantijų/maksimalaus srauto/Prioritetų dėliojimas 5.6.6.5.6. Minimalaus pralaidumo užtikrinimas; 5.6.6.5.7. Maksimalaus pralaidumo apribojimas; 5.6.6.5.8. Viršijančio srauto blokavimas (angl. trafficpolicing). 5.6.6.6. Srautų paskirstymas: 5.6.6.6.1. Srauto balansavimas pagal L3, L4 ir L7 OSI tinkle lygmenų informaciją; 5.6.6.6.2. HTTP session/cookie išsilaikymas; 5.6.6.6.3. Srauto paskirstymo metodas: statinis, pagal mažiausią sesijų skaičių (angl. roundrobin), pagal mažiausią atsako laiką (angl. roundtriptime) – weighted. 5.6.6.7. Sisteminiai įrašai / Stebėjimas: 5.6.6.7.1. Vidinis įvykių žurnalas; 5.6.6.7.2. Įvykių persiuntimas į nutolusį „Syslog“ serverį; 5.6.6.7.3. Grafinis realaus laiko ir istorinis stebėjimas; 5.6.6.7.4. SNMP; 5.6.6.7.5. E-mail įspėjimai apie virusus ir atakas; 5.6.6.7.6. VPN tunelių stebėjimas; 5.6.7. Turi būti atliekama ugniasienės priežiūra, apimanti bet neapsiribojanti šiais Tiekėjo darbais: 5.6.7.1. Ugniasienių incidentų sprendimas; 5.6.7.2. Įrangos programinės įrangos (angl. Firmware) sekimas ir atnaujinimų diegimas. Vykdoma ne rečiau kaip kartą per 3 mėnesius; 5.6.7.3. Ugniasienės aukšto patikimumo tikrinimas, kurio metu, suderinus su Pirkėju, yra išjungiamas telkinio pagrindinis (angl. master) įrenginys ir stebima, ar aktyvuojasi antrinis (angl. slave) įrenginys. Atliekama ne rečiau kaip 1 kartą per metus. 5.6.7.4. Ugniasienės proaktyvus stebėjimas. Stebimi fizinės/virtualios įrangos parametrai, mikrokodo parametrai, sisteminiai ir saugumo įrašai (angl. log). Atliekama ne rečiau kaip kartą per mėnesį; 5.6.7.5. Įrenginių konfigūracijų atsarginės kopijos sukūrimas kaskart atliekant konfigūracijos pakeitimus. 5.6.8. Tinklo nustatymų dokumentacijos atnaujinimas kaskart atliekant konfigūracijos pakeitimus. Dokumentuojami virtualių mašinų IP adresai, potinklų, VLAN, maršrutų (angl. gateway) ir kiti su Pirkėju suderinti duomenys. Atnaujinta dokumentacija ne rečiau kaip kas mėnesį turėtų būti teikiama Pirkėjui xlsx ar kitu suderintu formatu. 5.6.9. Įrenginių konfigūracijų teikimas Pirkėjui tekstiniu (xml, txt, json) ar kitu suderintu formatu (turi būti galima versijuoti GIT ar analogiškoje sistemoje). Atliekama ne rečiau kaip kartą per mėnesį. 5.6.10. Visos ugniasienės priežiūros sąnaudos turi būti įtrauktos į pasiūlymą. 5.6.11. Pagal Pirkėjo užsakymą turi būti atliekami administravimo (konfigūravimo) darbai: 5.6.11.1. DNS įrašų koregavimas; 5.6.11.2. Prievadų peradresavimo (Port Forward) konfigūravimas; 5.6.11.3. VPN kanalų konfigūravimas; 5.6.11.4. Ugniasienės taisyklių konfigūravimas; 5.6.11.5. Visi administravimo (konfigūravimo) darbai turi būti įskaičiuoti į paslaugų kainą.
--	---

5.7.	DR sprendimo testavimui keliami reikalavimai	5.7.1. DR procedūros turi būti testuojamos vieną kartą per metus, imituojant pilną DR aktyvavimą. 5.7.2. Turi būti suplanuotas produkcinės sistemos DR aktyvavimas Pirkėjo nurodytiems resursams. 5.7.3. Turi būti parengtos DR sprendimo aktyvavimo nuostatos bei sprendimo realizavimo planas. Už DR plano paruošimą ir jo testavimą yra atsakingas paslaugų Tiekėjas. 5.7.4. Po Paslaugos parengimo naudoti, ne vėliau kaip per 2 savaites turi būti atliktas IS avarinio perkėlimo testavimas ir patikrintas DRP išbaigtumas. 5.7.5. Atliekant pradinį bei pakartotinius DRP testavimus, aplikacijų testavimą po DR atliks Pirkėjas. 5.7.6. DR sprendimo DRP bandymo veiksmų plano realiomis sąlygomis paruošimas ir suderinimas su Pirkėju; 5.7.7. DR sprendimo testavimas pagal su Pirkėju suderintą grafiką ir planą; 5.7.8. Laukiamas DR sprendimo testavimo rezultatas turi būti aptartas ir iš anksto suderintas su Pirkėju. Neigiamą rezultatą parodęs testavimas turi būti pakartotas ne vėliau kaip per 1 mėnesį nuo rezultato patvirtinimo. 5.7.9. Esant poreikiui DR sprendimo testavimas gali būti kartojamas su Pirkėju suderintu laiku. 5.7.10. Testavimo rezultatai turi būti tinkamai dokumentuoti ir pateikti Pirkėjui iš anksto suderintos formos ataskaitoje.
Pagrindiniai teisės aktai, kuriais Tiekėjas privalo vadovautis		
5.8.	Bendrasis duomenų apsaugos reglamentas	
5.9.	Standartas LST ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“	
5.10.	Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas	
5.11.	Lietuvos Respublikos kibernetinio saugumo įstatymas	
5.12.	Bendrijų elektroninės informacijos saugos reikalavimų aprašas	
5.13.	Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas	
Reikalavimai Paslaugų vykdymui		
5.14.	5.14.1.	Tiekėjas turi atlikti paslaugoms teikti naudojamos virtualizacijos platformos programinės įrangos priežiūrą bei diegti atnaujinimus. Virtualizacijos platformos programinės įrangos saugumo ir kritinius atnaujinimus įdiegti nedelsiant, jeigu nėra žinomų faktų, jog atnaujinimai gali sutrikdyti paslaugų ir programinės įrangos veiklą. Atnaujinimų diegimo procedūra turi būti suderinta su Pirkėju.
	5.14.2.	Teikiant paslaugas Pirkėjui, turi būti naudojama tik legali programinė įranga.
	5.14.3.	Atsižvelgiant į nacionalinio kibernetinio saugos centro nurodymą, Tiekėjas privalo užtikrinti, kad teikiant paslaugas Pirkėjui nebūtų naudojama Kaspersky Lab programinė įranga ir kita nerekomenduojama naudoti programinė įranga.
	5.14.4.	Turi būti užtikrinamas patalpų, kuriose yra Pirkėjui pateikiama infrastruktūra, saugumas (apribojamas neįgaliojų asmenų pateikimas į atitinkamas patalpas ir kt.). Prieiga prie Pirkėjui pateikiamos infrastruktūros gali būti suteikiama tik tam asmeniui, kuriam prieiga reikalinga priskirtiems darbams atlikti.
	5.14.5.	Tiekėjas privalo užtikrinti, kad Pirkėjui skirti resursai (virtualios tarnybinės stotys, virtualus tinklas ir t.t.) bus programiškai atskirti nuo kitiems Tiekėjo klientams skirtų resursų.

	5.14.6. Tiekėjas turi užtikrinti, kad Pirkėjo paslaugoms skirti duomenų centro komponentai fiksuotą šią informaciją: įjungimą, išjungimą, sėkmingus, nesėkmingus bandymus registruotis prie jų bei kitus saugai svarbius įvykius, nurodant saugai svarbaus įvykio ar įvykdyto veiksmo identifikatorių ir laiką. Turi būti užtikrinta žurnalinių įrašų apsauga nuo nesankcionuoto ar tyčinio pakeitimo, ar sunaikinimo. 5.14.7. Pirkėjas turi turėti galimybę peržiūrėti Pirkėjo paslaugoms skirtų duomenų centro komponentų žurnalinius įrašus bei esant poreikiui, gauti Pirkėjo paslaugoms skirtų duomenų centro komponentų žurnalinių įrašų kopiją. 5.14.8. Tiekėjas privalo užtikrinti, kad jo naudojamame duomenų centre esantys Pirkėjo duomenys ir jų kopijos būtų neprieinamos nei fiziniu būdu, nei kitokiais būdais atitinkamų įgaliojimų neturintiems asmenims ar trečiosioms šalims. 5.14.9. Tiekėjas privalo užtikrinti, kad be raštiško Pirkėjo sutikimo Pirkėjo duomenys ir jų kopijos nebus perkeltos į kitą duomenų centrą ar lokaciją. 5.14.10. Tiekėjas privalo turėti ekstremalių situacijų Tiekėjo duomenų centruose valdymo planą (-us). Pirkėjui pareikalavus turi būti sudarytos sąlygos susipažinti su šiuo planu. 5.14.11. Tiekėjas privalo nedelsiant, ne vėliau nei per 8 val. nuo incidento pradžios, iš anksto suderintu būdu informuoti Pirkėją apie duomenų centro infrastruktūroje įvykusius kibernetinius incidentus ir jų poveikį Pirkėjo IS. Incidentai apie kurios būtina pranešti: 5.14.11.1. Informacijos vientisumo, konfidencialumo ar laukiamo prieinamumo pažeidimus; 5.14.11.2. Žmogaus klaidas; 5.14.11.3. Saugos politikų ar gairių nesilaikymą, prieigos pažeidimus; 5.14.11.4. Fizinio saugumo susitarimų pažeidimus; 5.14.11.5. Nekontroliuojamus sistemos pakeitimus; 5.14.11.6. Programinės įrangos arba aparatinės įrangos pažeidimus ir trikdžius. 5.14.12. Išsprendus incidentą, Tiekėjas turi užpildyti ir suderintu būdu, ne vėliau nei per 3 d. d. po incidento išsprendimo, pateikti kibernetinio incidento tyrimo ataskaitą. 5.14.13. Pirkėjui pareikalavus per sutartą laiką turi būti sudarytos sąlygos susipažinti su informacija, kaip yra laikomasi šio Pirkimo bei teisės aktuose numatytų reikalavimų, kokios ir kaip yra taikomos techninės bei organizacinės paslaugų teikimo ir duomenų saugos priemonės.
Paslaugų teikimo sąlygos	
5.15.	5.15.1. Paslaugų aptarnavimas darbo dienomis ir savaitgaliais (0:00-24:00), reakcija į užklausą/ sprendimas: 1 val./4 val. 5.15.2. Visų teikiamų Paslaugų valdymo organizavimui Tiekėjas turės: 5.15.2.1. Užtikrinti tinkamą paslaugų organizavimą, apibrėžiant vadovavimo, valdymo ir vykdymo atsakomybes ir atsiskaitymo būdus; 5.15.2.2. Paskirti projekto vadovą, kuris bus atsakingas už darbų organizavimą, koordinavimą ir derinimą su Pirkėjo įgaliojais atstovais. 5.15.2.3. Pirkėjo įgalioti atstovai, registruodami pranešimą pagalbos sistemoje, pranešimui priskiria tipą (užklausa, sutrikimas, keitimas) ir, priklausomai pranešimo tipo, nustatoma sprendimo įvykdymo trukmė. 5.15.2.4. Turi būti taikomi tokie Paslaugų parametrai: 5.15.2.4.1. Kritinis sutrikimas. Visiškas arba dalinis Paslaugų sutrikimas, kai visai arba iš dalies neįmanoma atlikti tam tikrų funkcijų arba šių funkcijų pateikiami rezultatai yra klaidingi. Problemos sprendimas yra būtinas skubiai. Sutrikimo šalinimo laikas – ne ilgiau kaip 4 valandos; 5.15.2.4.2. Sutrikimas. Veiklos procesai ir Paslaugų funkcionavimas paveiktas nežymiai, sutrikimas nekelia grėsmės duomenims ir Paslaugų funkcionavimui, problemos sprendimas yra būtinas, bet ne kritinis. Sutrikimo šalinimo laikas – ne ilgiau kaip 8 valandos. 5.15.2.4.3. Užklauskos ir keitimai. Išsprendimo laikas - ne ilgiau kaip konkrečiai užklauskai/keitimui išspręsti reikalingas ir Tiekėjo su Pirkėju individualiai suderintas laikas. 5.15.3. Sutrikimo, užklauskos ir keitimo išsprendimo laikas – tai laikas nuo momento, kai Pirkėjas praneša Tiekėjui apie sutrikimą, užklausą ar keitimą, iki momento, kai Tiekėjas atliko visus būtinus užklauskos įgyvendinimui darbus ir fiksavo tai Pagalbos sistemoje.

	5.15.4.	Į sutrikimo, užklauso ar keitimo išsprendimo laiką neįskaičiuojamas laikas, kai Tiekėjas negali vykdyti su išsprendimu susijusios veiklos dėl ne nuo Tiekėjo priklausančių aplinkybių. Apie tokias aplinkybes Tiekėjas turi informuoti Pirkėją.
	5.15.5.	Jeigu užklauso, keitimo ar sutrikimo neįmanoma išspręsti per nustatytą pašalinimo laiką, Tiekėjas privalo iš anksto apie tai informuoti Pirkėją.
	5.15.6.	Nesilaikant nustatytų ir/arba suderintų išsprendimo laikų, nurodytų 5.15.1. ir 5.15.2.4. punktuose, Tiekėjas privalės mokėti 100 Eur dydžio baudą už kiekvieną pavėluotą valandą.
	5.15.7.	Per pirmas tris dienas po sutarties įsigaliojimo baudos nebus taikomos už sutrikimų šalinimo laikus, kurių bendra išsprendimo trukmė ne ilgesnė kaip 8 val.
Bendrieji reikalavimai		
5.16.	5.16.1.	Jeigu Tiekėjui parengti pasiūlymą neužtenka techninėje specifikacijoje pateiktos informacijos, Tiekėjas gali atvykti į objektą ir pilnai įsivertinti reikalaujamas atlikti darbų apimtis. Visos išlaidos susijusios su objekto apžiūra yra išskirtinai Tiekėjo sąskaita.
	5.16.2.	Paslaugų rezultatai turi būti gaunami, naudojant šiuos metodus – interviu, teisės aktų ir vidinių dokumentų analizę, fizinę ir loginę apžiūrą.
	5.16.3.	Pateikti dokumentaciją pagal Pirkėjo pateiktus (jei Pirkėjas juos pateikia) arba su Pirkėju suderintus dokumentų pavyzdžius ar šablonus.
Paslaugų teikimo metu Tiekėjas privalo Paslaugų teikimą planuoti taip, kad:		
5.17.	5.17.1.	Būtų maksimaliai užtikrinta, kad nenukentės Pirkėjo šiuo metu vykdoma veikla.
	5.17.2.	Tiekėjas ir jo darbuotojai vykdysiantys sutartį, privalo pasirašyti Konfidencialios informacijos ir jos neatskleidimo pasižadėjimą (Sutarties 2 priedas). Konfidencialia informacija laikoma įskaitant, bet neapsiribojant: asmens duomenys, vartotojų prisijungimo duomenys, serverių ir kitų informacinių išteklių ir įrangos IP adresai, vardai, informacinių išteklių sąranka, vartotojų ir informacinių išteklių duomenys, serveriuose ir darbo vietose saugojama informacija.

6. PIRKIMO OBJEKTO APIMTYS

6.1. Taikoma kainodara:

☒ Fiksuotas įkainis

6.2. Nurodytas maksimalus planuojamas įsigyti kiekis. Sutarties kaina yra lygi Tiekėjo pasiūlymo kainai be PVM, apskaičiuotai sudauginus maksimalų paslaugų kiekį iš Tiekėjo pasiūlyto įkainio (-ių) be PVM.

Eil. Nr.	Pavadinimas	Mato vnt.	Maksimalus kiekis
1.	IS avarinio perkėlimo ir atstatymo (toliau – DR) rezerviniame duomenų centre (DRaaS) paslaugos	mėn.	30
2.	Ugniasienės FWaaS paslaugos	mėn.	30
3.	Duomenų perdavimo tinklo paslaugos	mėn.	30
4.	Atstatymo po avarijos plano (toliau - DRP) paruošimo ir jo testavimo paslaugos	mėn.	30

Sutarties galiojimo laikotarpiu Pirkėjas turi teisę koreguoti perkamą kiekį neviršijant nurodyto maksimalaus kiekio ir maksimalios sutarties kainos.

☒ Pirkėjas įsipareigoja įsigyti ir apmokėti visus minimalius specifikacijoje nurodytus rezervuotus resursus nuo Paslaugos teikimo pradžios momento, nepriklausomai nuo faktinio jų naudojimo ar aktyvavimo datos.

☒ Pirkėjas turi teisę įsigyti Sutartyje nenumatytas, tačiau su pirkimo objektu / Sutarties dalyku susijusias paslaugas (toliau – **nenumatytos paslaugos**), kurių bendra vertė per visą Sutarties galiojimo laikotarpį negali viršyti 10 procentų Sutarties kainos. Nenumatytų paslaugų įsigijimų kaina turi būti įskaičiuota į Sutarties maksimalią kainą. **Sutarties maksimalia kaina laikoma Sutarties kaina su 10 procentų nenumatytais paslaugoms.**

7. KARTU SU PASIŪLYMU PATEIKIAMAI DOKUMENTAI

EIL. NR.	PAVADINIMAS
7.1.	Jeigu duomenų centras įrengtas ne pagal 5.4.3. punkte nurodytą reikalavimą, Tiekėjas turi pateikti nepriklausomos kompetentingos institucijos išduotą dokumentą, įrodantį, kad duomenų centras yra apsaugotas nuo vandens poveikio (užliejimo) įvykus stichinėms nelaimėms arba avarijoms šalia esančiuose inžineriniuose tinkluose.
7.2.	„Tier III Design“ ir „Tier III Facility“ arba lygiaverčiai sertifikatai, išduoti Tiekėjo duomenų centrui.
7.3.	5.5.5 punkte nustatytu atveju Tiekėjas teikia laisvos formos aprašymą, kaip pasirinktos technologijos atitinka visus šiame dokumente aprašytus Pirkėjo reikalavimus, ypač saugos, paslaugų kokybės (QoS), QoS bendravimo (interworking) visose naudojamų technologijų lygmenyse ir kaip Tiekėjas ketina jas įgyvendinti.
7.4.	Kai Tiekėjas ketina remtis subtiekejų ar kitų ūkio subjektų infrastruktūra, kartu su pasiūlymu privalo pateikti informaciją, kuri (-ios) tinklo dalis (-ys) priklauso subtiekejams ar kitiems ūkio subjektams, įvardinant tinklo atkarpas ir jų savininkus, ir/arba kuri siūlomo duomenų perdavimo tinklo dalis (infrastruktūra) yra Tiekėjo nuosavybė.
7.5.	Duomenų centrų ir juose esančios techninės įrangos, ryšio linijų nuosavybės dokumentai.

8. SUTARTIES VYKDYMO METU TEIKIAMAI DOKUMENTAI

EIL. NR.	PAVADINIMAS	TEIKIMO MOMENTAS
8.1.	Esamos infrastruktūros DR sprendimo diegimui įvertinimas ir detalios aprašytas Paslaugos diegimo metodas ir diegimo darbų grafikas	Per 10 dienų po sutarties pasirašymo
8.2.	Paslaugų, kurioms teikiamas DR spendimas, sąrašas (pavadinimai, resursai, tinklo parametrai, versijos ir t.t.)	Per 14 dienų po sutarties pasirašymo
8.3.	Ryšų tarp įrenginių diagrama ir lentelė	Per 14 dienų po sutarties pasirašymo
8.4.	Tinklo topologija ir infrastruktūrinių paslaugų (pvz.: DNS, AD, LB, WAF ir t.t.) sąrašas	Per 20 dienų po sutarties pasirašymo
8.5.	Sudarytos ir suderintos Rezervinio duomenų kopijavimo ir atstatymo po avarijos taisyklės	Po Paslaugos įdiegimo ir parengimo aktyvavimui
8.6.	DR sprendimo aktyvavimo nuostatos bei sprendimo realizavimo planas	Po Paslaugos įdiegimo ir parengimo aktyvavimui
8.7.	Sistemų avarinio atstatymo planas (Failover plan).	Po Paslaugos įdiegimo ir parengimo aktyvavimui
8.8.	Sistemų grąžinimo į Pirkėjo duomenų centrą planas (Failback plan).	Po Paslaugos įdiegimo ir parengimo aktyvavimui
8.9.	Sudarytas ir suderintas Nuotolinių prisijungimų sprendimo aprašymas	Po Paslaugos įdiegimo ir parengimo aktyvavimui
8.10.	Paslaugos priėmimo-perdavimo aktai	Po Paslaugos įdiegimo ir parengimo aktyvavimui
8.10	DR sprendimo pilno DRP testavimo realiomis sąlygomis ataskaita	Per 60 dienų po Paslaugos įdiegimo ir paruošimo naudoti.

9. SUTARTINIŲ ĮSIPAREIGOJIMŲ VYKDYMO VIETA

☒ Tiekėjo buveinėje.

10. PASLAUGŲ TEIKIMO TVARKA IR TERMINAI

10.1. Paslaugų teikimo terminai

Bendras paslaugų teikimo terminas - 30 (trisdešimt) mėnesių nuo Sutarties pasirašymo dienos.

10.2. Užsakymų teikimo tvarka

☒ El. paštu

11. KOKYBĖ IR TRŪKUMŲ ŠALINIMAS

11.1. Sutarties vykdymo ar garantinio termino metu pastebėtiems trūkumams šalinti nustatomas 3 (trijų) mėnesių terminas nuo Pirkėjo pranešimo apie nekokybiškas paslaugas išsiuntimo el. paštu Teikėjui momento.

12. PRIEDAI

Priedas Nr. 1. Nacionalinio saugumo reikalavimų atitikties deklaracija (VPT BVPŽ).