

DEBESŲ KOMPIUTERIJOS, KOMPIUTERINIŲ TINKLŲ IR VIRTUALIŲ STOČIŲ PRIEŽIŪROS PASLAUGŲ TEIKIMO TECHNINĖ SPECIFIKACIJA

1. PIRKIMO OBJEKTAS

BALTPOOL UAB (toliau – *Pirkėjas*) perka debesų kompiuterijos, kompiuterinių tinklų ir virtualių stočių priežiūros paslaugas (toliau – *Paslaugos*). Perkamas Paslaugas sudaro:

- Dedikuotos tarnybinės stotys;
- Techninė įranga kaip paslauga (angl. *Infrastructure as a Service – IaaS*);
- Programinės įrangos platforma kaip paslauga (angl. *Platform as a Service – PaaS*);
- Vietinis IT palaikymas kaip paslauga (angl. *Local Support as a Service – LSaaS*);
- Susitarimas dėl paslaugos lygio (angl. *Service-level agreement SLA*);
- Nutolusi rezervinės kopijos paslauga už Lietuvos Respublikos ribų;
- Konsultavimas kaip paslauga (angl. *Competence as a Service – CaaS*) pirkimo objekto apimtyje (tarnybinės stotys, virtualizavimo platforma, duomenų apdorojimo ir saugojimo resursai, sisteminė ir standartinė programinė įranga, šviesolaidinės duomenų perdavimo linijos, rezervinio kopijavimo užtikrinimas, infrastruktūros priežiūra ir valdymas).

2. SĄVOKOS IR APIBRĖŽIMAI

Sąvokos	Aprašymas
Paslaugų teikimo laikas	Laiko periodas, kurio metu užtikrinamas Paslaugų funkcijų teikimas.
Paslaugų palaikymo valandos	Laiko periodas, kai sprendžiami Paslaugų incidentai ir vykdomos užklauskos ir kiti su Paslaugų teikimu susiję darbai.
Kreipinys	Paslaugų naudotojo pranešimas apie atsiradusius incidentus, užklauskas ar keitimus.
Incidentas	Paslaugų teikimo sutrikimas, dėl kurio Paslaugos tampa Pirkėjui nepasiekiamos arba sutrinka bent viena iš Paslaugų funkcijų.
Užklausa	Pirkėjo prašymas atlikti administravimo darbus, nesusijusius su incidento šalinimu.
Keitimas	Paslaugų, konfigūracijos elemento, proceso ar dokumento ir kt., kas gali įtakoti Paslaugų teikimą, papildymas, pakeitimas ar pašalinimas.
Reakcijos laikas	Laikotarpis, per kurį Pirkėjo kreipinys yra užregistruojamas ir pradedamas spręsti.
Sprendimo laikas	Laikotarpis, nuo kreipinio užregistravimo iki jo išsprendimo: (i) incidentams, tai pilnas Paslaugų funkcijų atstatymas; (ii) užklauskoms, tai laikas iki užduoties pilno įvykdymo.
DBVS	Duomenų bazių valdymo sistema

KDV	Kompiuterinės darbo vietos
Tarnybinės stoties duomenys	Visi failai, esantys tarnybinėje stotyje, įskaitant informacinių sistemų duomenų failus ir naudotojų failus.
Paslaugų pasiekiamumas	Paslaugų pasiekiamumas yra paskaičiuojamas iš „viso valandų Paslaugų tiekimo laiko per mėnesį“ (toliau - TL) atimant „viso valandų, kai nebuvo teikiamos Paslaugų funkcijos, per mėnesį“ (toliau – NF) ir gautą skaičių padalinant iš „viso valandų Paslaugų tiekimo laiko per mėnesį“ bei gautą skaičių padauginant iš 100: $\text{Pasiekiamumas, \%} = \frac{\text{TL} - \text{NF}}{\text{TL}} \times 100$

3. PIRKIMO OBJEKTO APIMTYS

Eil. Nr.	Pavadinimas	Mato vnt.	Preliminarus kiekis per mėn.	Trukmė, mėn.
Tarnybinių stočių ir kitų infrastruktūros resursų paslaugos				
1.	Virtualūs procesoriai (vCPU)	vnt.	80	36
2.	Operatyvinė atmintis (RAM)	GB	120	36
3.	Duomenų saugykla (SSD)	GB	2000	36
4.	Duomenų centre dedikuotas interneto kanalas 1 Gbps	vnt.	1	36
5.	Duomenų saugykla, rezervinė kopija	GB	2000	36
6.	Papildomas atsarginių kopijų saugojimas nutolusiame DC	GB	2000	36
7.	Užsakovo VPN sujungimas su DC, 100 Mbps pralaidumu	GB	1	36
8.	Užsakovo LAN sujungimas su DC LAN (Lan-to-Lan), 1 Gbps pralaidumu	GB	1	36
9.	Virtualaus maršrutizatorius Tiekėjo duomenų centre	vnt.	1	36
10.	Ugniasienės nuoma	vnt.	1	36
11.	Tiesioginis sujungimas (VPN) tarp Pirkėjo ir Valstybinės mokesčių inspekcijos	vnt.	1	36
12.	Viešas interneto adresas (WAN IP)	vnt.	12	36
13.	Migravimo darbai į Tiekėjo duomenų centrą	vnt.	1	1
14.	Konsultacijos ir papildomi darbai	vnt.	1	36

15.	MS Windows Server operacinės sistemos licencija	vnt.	5	36
Virtualių stočių priežiūros ir vietinio kompiuterio tinklo priežiūros paslaugos				
16.	Linux Serverio OS priežiūra	vnt.	10	36
17.	Windows Serverio OS priežiūra	vnt.	4	36
18.	Virtualaus maršrutizatoriaus Tiekėjo duomenų centre priežiūra	vnt.	1	36
19.	Ugniasienės priežiūra	vnt.	1	36
20.	Vietinio kompiuterinio tinklo (1 vnt. maršrutizatorius, 1 vnt. komutatorius, 2 vnt. WiFi AP) priežiūra	vnt.	1	36

3.1. Nurodytas Paslaugų kiekis yra orientacinis. Pirkėjas neįsipareigoja nupirkti viso nurodyto Paslaugų kiekio. Nurodytas preliminarus Paslaugų kiekis gali keistis priklausomai nuo Pirkėjo poreikio.

3.2. Paslaugų teikimo metu gali būti prašoma suteikti su Paslaugom susijusias konsultacijas. Suteiktos konsultacijos apmokamos pagal faktą pasibaigus einamajam kalendoriniam mėnesiui ir pasirašius perdavimo-priėmimo aktą. Konsultacijų kaina nustatoma pagal Tiekėjo pasiūlyme nurodytas atitinkamas darbo valandos kainas (įkainius).

3.3. Tiekėjas turi užtikrinti Lietuvos Respublikoje registruotų ir veikiančių ryšio operatorių prijungimą, vienodomis techninėmis ir finansinėmis sąlygomis, prie nuomojamos įrangos, pagal Pirkėjo poreikius.

3.4. Siūlomoje kompiuterinėje infrastruktūroje, turi būti galimybė kurti virtualius tinklus (VLAN).

3.5. Paslaugos turi būti diegiamos ir konfigūruojamos taip, kad bet kuriuo metu Pirkėjo sistema ir duomenys galėtų būti perkelti į kitą Pirkėjo nurodytą duomenų centrą. Paslaugų teikimui turi būti naudojama standartinė kompiuterinė ir programinė įranga, plačiai naudojama duomenų centruose.

4. REIKALAVIMAI PAGALBOS TARNYBAI

Eil. Nr.	Charakteristika	Reikalavimai
1.	Darbo laikas	Tiekėjas turi turėti 24 valandas per parą ir 7 dienas per savaitę (toliau – 24x7) veikiančią pagalbą tarnybą.
2.	Kalba	Tiekėjas turi turėti pagalbą tarnybą, kurioje komunikavimas su Pirkėju vykėtų lietuvių kalba tiek raštu, tiek žodžiu.
3.	Komunikacijos kanalai	Tiekėjo pagalbą tarnyba turi suteikti galimybes registruoti kreipinius įvairiais nurodytais kanalais: elektroniniu paštu; fiksuoto ir mobilaus ryšio telefonu; naudojant WEB sąsają.
4.	Metodika	Tiekėjas turi būti įdiegęs veikiančius ir aprašytus incidentų bei keitimų valdymo procesus, atitinkančius IT paslaugų valdymo (ITIL ar analogiškos metodikos) gerųjų praktikų rekomendacijas bei veikiančią Tiekėjo pagalbą tarnybos interneto svetainę (portalą) kreipiniams registruoti bei peržiūrėti.

5.	Informacijos pateikimas	Tiekėjo pagalbos tarnyba turi užtikrinti operatyvų atgalinį ryšį ir informacijos apie incidentus realiu laiku (angl. <i>On-line</i>) teikimą Tiekėjo pagalbos tarnybos interneto svetainėje, veikiančioje HTTPS protokolu.
6.	Informavimas	Tiekėjo pagalbos tarnyba turi automatiškai (pvz. el. laiško pranešimu) informuoti Pirkėjo nurodytus darbuotojus apie užregistruotų incidentų statusą, planuojamą incidentų išsprendimo datą ir laiką bei incidentų išsprendimą.

5. REIKALAVIMUI DUOMENŲ CENTRUI

Eil. Nr.	Charakteristika	Reikalavimai
1.	Lokacija	Duomenų centras turi būti įrengtas Europos Sąjungos arba šalies, priklausančios NATO, teritorijoje (pasiūlyme nurodyti tikslų adresą).
2.	Duomenų centras turi turėti TIER III ar lygiavertę sertifikaciją ir tai įrodančius dokumentus	Turi būti pateikiama: • Tier 3 Facility ar lygiavertė • Tier 3 Design ar lygiavertė
3.	Duomenų centras	• Duomenų centras neturi būti įrengtas požeminiame ar paskutiniame pastato aukšte. Jei duomenų centras įrengtas ne pagal nurodytą reikalavimą, tai Tiekėjas kartu su pasiūlymu 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. • Tarnybinių stočių ir kitos technologinės duomenų centro patalpos (nepertraukiamo maitinimo šaltinių, oro kondicionavimo įrenginių, dujų gesinimo sistemos) negali turėti langų. • Tarnybinių stočių patalpa turi būti atspari ugnies ir vandens poveikiui. • Duomenų centro patalpose turi būti įrengta vaizdo stebėjimo sistema su įrašymo funkcija. • Duomenų perdavimo tinklo ir elektros tinklo kabeliai turi būti atskirti ne mažesniu nei 1 m atstumu. • Tarnybinių stočių laikymo patalpoje turi būti įrengta tikslaus klimato kontrolės sistema, palaikanti pastovią temperatūrą 20-23°C ir drėgnumą 40-60% ribose. • Tikslaus klimato kontrolės sistema turi būti dubliuota mažiausiai N+1 lygiu. • Tarnybinių stočių ir nepertraukiamo maitinimo šaltinio patalpose turi būti įrengta priešgaisrinė signalizacija. • Tarnybinių stočių ir nepertraukiamo maitinimo šaltinio patalpose turi būti įrengtos autonominės nepriklausomos gesinimo dujomis sistemos.

		• Elektros tiekimas į duomenų centrą turi būti užtikrinamas 2 nepriklausomomis įvadinėmis linijomis. • Elektros srovės nepertraukiamas tiekimas tarnybinių stočių patalpai turi būti užtikrintas nepertraukiamo maitinimo šaltinio sistemos pagalba. • Nepertraukiamo maitinimo šaltinio sistema turi būti dubliuota mažiausiai N+1 lygiu. • Tarnybinių stočių, duomenų saugyklų, kompiuterinio tinklo įrangos, naudojamos Paslaugų teikimui iš duomenų centro, maitinimas turi būti dubliuotas N+1 lygiu. • Duomenų centras turi turėti autonominį elektros srovės generatorių, užtikrinantį nepertraukiamą duomenų centro sistemų veikimą 72 valandas, esant maksimaliam jo apkrovimui. • Tarnybinių stočių patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas, įrengti gaisro ir įsilaužimo davikliai, kurių stebėsena ir kontrolė turi būti užtikrinama 24 valandas per parą. • Patekimas į tarnybinių stočių patalpas turi būti griežtai reglamentuotas ir patvirtintas Tiekėjo vidaus tvarkos taisyklėmis, užtikrinant visapusę patenkančių asmenų atsakomybę, kontrolę ir palydą.
--	--	---

6. REIKALAVIMAI NUTOLUSIAM DUOMENŲ CENTRUI

Eil. Nr.	Charakteristika	Reikalavimai
1.	Lokacija	Duomenų centras turi būti įrengtas Europos Sąjungos arba šalies, priklausančios NATO, teritorijoje (pasiūlyme nurodyti tikslių adresą).
2.	Atstumas iki duomenų centro	Turi būti nutolęs ne mažiau kaip 800 km nuo siūlomo pagrindinio duomenų centro.
3.	Duomenų centras	Duomenų centras neturi būti įrengtas požeminiame ar paskutiniame pastato aukšte. Jei duomenų centras įrengtas ne pagal nurodytą reikalavimą, tai Tiekėjas kartu su pasiūlymu 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.
4.	Apsauga	• Patekimas į duomenų centro teritoriją ir patį duomenų centrą turi būti kontroliuojamas 24x7. • Turi būti užtikrinama žmogiška apsauga 24x7. • Visa teritorija turi būti filmuojama, o įrašai saugomi.
5.	Elektra	• Elektros tiekimas į duomenų centrą turi būti užtikrinamas 2 nepriklausomomis įvadinėmis linijomis. • Elektros srovės nepertraukiamas tiekimas tarnybinių stočių patalpai turi būti užtikrintas nepertraukiamo maitinimo šaltinio sistemos pagalba.

		• Nepertraukiamo maitinimo šaltinio sistema turi būti dubliuota mažiausiai N+1 lygiu.
6.	Klimato kontrolė	• Tarnybinių stočių laikymo patalpoje turi būti įrengta tikslaus klimato kontrolės sistema pagal ASHRAE arba lygiavertį standartą, palaikanti pastovią temperatūrą ir drėgnumą, bet ne blogiau kaip 18-27 °C ir drėgnumą 40-60% ribose. • Tikslaus klimato kontrolės sistema turi būti dubliuota mažiausiai N+1 lygiu.

7. REIKALAVIMAI RYŠIO PASLAUGOMS IKI NUTOLUSIO DUOMENŲ CENTRO

Eil. Nr.	Charakteristika	Reikalavimai
1.	Paslaugų teikimo laikas	24x7
2.	Paketų praradimas	Ne didesnis kaip 1%.
3.	Persiųstų-gautų duomenų kiekis	Neturi būti papildomai apmokestinamas.
4.	Ryšio linijos	Nutolės duomenų centras turi būti pasiekiamas dviem dubliuotais ryšio kanalais ne mažesne kaip 1 Gbps „full duplex“ sparta (išsiuntimas/parsiuntimas).
5.	Internetas nutolusiame duomenų centre	Ne mažesne kaip 1 Gbps „full duplex“ sparta (išsiuntimas/parsiuntimas).

8. REIKALAVIMAI VIRTUALIŲ TARNYBINIŲ STOČIŲ RESURSŲ NUOMOS PASLAUGOS TEIKIMUI

Eil. Nr.	Charakteristika	Reikalavimai
1.	Paslaugų teikimo užtikrinimas	Paslaugos, visą jos teikimo laikotarpį, turi apimti visą jai 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 paslaugos teikimu susijusias sąnaudas.
2.	Platforma	Siūlomos virtualizacijos platformos gamintojo išduotas įgaliojimas arba kitas lygiavertis dokumentas, patvirtinantis, jog Tiekėjas yra oficialus gamintojo atstovas, turintis teisę naudoti programinės įrangos licencijas. Pateikiami dokumentai tiesiogiai suformuoti elektroninėmis priemonėmis arba skaitmeninės dokumentų kopijos.
3.	Licencijavimas	Tiekėjas turi turėti teisę nuomoti pirkimo techninėje specifikacijoje nurodytą Microsoft, kaip ir Paslaugų gavėjo naudojamą, programinę įrangą, įdiegtą jo duomenų centre. Tiekėjas, teikdamas pasiūlymą turi pateikti nuomojamos programinės įrangos gamintojo ar oficialaus jo atstovo išduotą dokumentą, patvirtinantį Tiekėjo teisę nuomoti siūlomą

		programinę įrangą, įdiegtą jo duomenų centre arba „Microsoft Service Provider License Agreement (SPLA)“ duomenų centrų licencijavimo sutartis ar lygiavertę sutartį ir (ar) kitus šį reikalavimą patvirtinančius dokumentus.
4.	Paslaugų teikimo pradžia	Tiekėjas turi pradėti teikti paslaugą pagal žemiau aprašytas charakteristikas ir techninius reikalavimus ne vėliau kaip per 10 (dešimt) darbo dienų po sutarties pasirašymo.
5.	Paslaugų teikimo laikas	24x7
6.	Paslaugos pasiekiamumas	Ne blogiau kaip 99,5% per mėnesį, Pirkėjo nustatytu laiku – darbo dienomis nuo 7 valandos iki 19 valandos. Ne blogiau kaip 99% per mėnesį, kitu laiku.
7.	Paslaugos kokybės reikalavimai	• Reakcijos į incidentus laikas: ne ilgiau kaip 15 minučių. • Incidentų išsprendimo laikas: ne ilgiau kaip 4 valandos; • Reakcijos į užklausas ir keitimus laikas: ne ilgiau kaip 1 valanda. • Užklausų ir keitimų išsprendimo laikas: ne ilgiau kaip 8 valandos.
8.	Atitikimo kokybės reikalavimams ataskaita	Tiekėjas privalo pateikti paslaugų kokybės parametrų ataskaitą už praėjusį mėnesį, jeigu to reikalauja Pirkėjas. Ataskaitoje nurodomi šie duomenys: • Vidutinės incidentų reakcijos bei išsprendimo trukmės; • Visų incidentų sąrašas su nurodytais reakcijos bei išsprendimo laikais; • Mėnesio paslaugos pasiekiamumas; • Detalus saugumo incidentų sąrašas; • Informacija apie realų resursų naudojimą, pagal stebimus parametrus.
9.	Savitarnos portalas	Tiekėjas, teikdamas paslaugą, turi suteikti Pirkėjui savitarnos portalą, kuris turi leisti Pirkėjui savarankiškai atlikti tokius veiksmus: • Kurti, stabdyti, perkrauti, ištrinti virtualias tarnybines stotis; • Dinamiškai keisti visus virtualios tarnybinės stoties parametrus vCPU, RAM, HDD; • Virtualiai tarnybinei stočiai priskirti ne mažiau kaip 2 virtulius tinklo adapterius; • Kurti virtualias tarnybines stotis iš paruoštų šablonų; • Kurti virtualias tarnybines stotis pasinaudojant virtualiais ISO atvaizdais; • Kurti ir saugoti momentines virtualių tarnybinių stočių kopijas (angl. <i>Snap Shots</i>); • Turi būti galimybė pasinaudojant savitarnos portalu prisijungti prie virtualios tarnybinės stoties, nenaudojant papildomų programinių įrankių. Virtuali tarnybinė stotis turi būti pasiekama ir tuo atveju, kai jai nėra prijungtas ar suteiktas virtualus tinklo adapteris ar IP adresas.
10.	VLAN tinklai	Turi būti suteiktos 2 grupės VLAN (vidinis ir išorinis tinklas) tinklų, kad savitarnos portalo naudotojas galėtų dinamiškai

		valdyti ir priskirti virtualias tarnybines stotis į reikiamus tinklus ir potinklius.
11.	Palaikomos operacinės sistemos	Tarnybinių stočių virtualizavimo platformos turi palaikyti šias operacines sistemas, apimant bet neapsiribojant: Microsoft Windows Server 2012/2016/2022, Debian 8.x-11.x, Ubuntu 16.x-24.x Linux ar kitas lygiavertes.
12.	Licencijos	Tiekėjas turi užtikrinti įdiegtų virtualių tarnybinių stočių ir ugniasienių operacinių sistemų legalumą. Visas reikiamas licencijas legalumui užtikrinti be papildomo mokesčio pateikia Tiekėjas.
13.	Resursų stebėjimas	Tiekėjas atlieka veikiančių virtualių tarnybinių stočių stebėseną, stebi pasirinktus paslaugos teikimo/našumo parametrus, kurie turi būti suderinti su Pirkėju, taip pat Tiekėjas privalo teikti rekomendacijas dėl resursų išnaudojimo.
14.	Paslaugos funkcijos	Virtualių tarnybinių stočių veikimas. Galimybė kurti ne mažiau kaip 100 vnt. naujų operacinių sistemų aplinkų (angl. <i>Operating System Environment</i>). Galimybė didinti ir mažinti kiekvienai virtualiai tarnybinei stočiai skiriamus resursus (vCPU, RAM, HDD). Galimybė vienai virtualiai tarnybinei stočiai priskirti iki 24 vnt. virtualių procesorių. Visos virtualios tarnybinės stotys turi turėti galimybę užsikrauti naudojant pagrindinį įkrovos įrašą (angl. <i>Master Boot record (MBR)</i>) ir (arba) visuotinai unikalų identifikatorių skaitinių lentelėje (angl. <i>Globally unique identifier partition table (GUID partition table (GPT))</i>).
15.	Našumo ir pajėgumo parametrai	Ne mažiau nei 3 fizinės tarnybinės stotys, skirtos tarnybinių stočių virtualizavimo platformai. Jos turi būti apjungtos į aukšto patikimumo blokinį (angl. <i>cluster</i>). Fizinių tarnybinių stočių, skirtų tarnybinių stočių virtualizavimo platformai, procesorių našumas 2 procesorių aparatinėje platformoje 1 branduoliui ne mažiau negu 2200 matuojamųjų vienetų pagal: https://www.cpubenchmark.net/singleThread.html Suminis fizinių tarnybinių stočių operatyvinės atminties kiekis (RAM) ne mažesnis nei 1024 GB. Fizinių tarnybinių stočių, skirtų tarnybinių stočių virtualizavimo platformai, resursų (CPU ir RAM) panaudojimas neturi viršyti 70%.
16.	Duomenų saugyklų našumo parametrai	Duomenų saugyklos parametrai turi būti ne blogesni kaip: • Visi komponentai dubliuojami, įskaitant: - Ne mažiau kaip 2 valdymo moduliai; - Ne mažiau kaip 2 maitinimo šaltiniai. • Duomenų vientisumui neturi turėti įtakos pavieniai duomenų saugyklos kietųjų diskų gedimai. • Duomenų saugykla su fizinėmis tarnybinėmis stotimis turi būti sujungta ne blogesne nei: iSCSI arba FC sąsaja, kurios greیتaveika ne mažiau kaip 16 Gbps. Reikalavimai našumui: - Nuoseklus skaitymas - 1600 MB/s; - Nuoseklus rašymas - 1600 MB/s.

17.	Duomenų saugyklų našumo tipai	Virtualių tarnybinių stočių diskinės posistemės našumas turi būti ne mažesnis nei: 1000 IOPS (įvesties/išvesties operacijų kiekis per sekundę) 1TB naudojamos saugyklos vietos.
-----	-------------------------------	---

9. REIKALAVIMAI VIRTUALIŲ TARNYBINIŲ STOČIŲ KOPIJAVIMO IR ATSTATYMO PASLAUGOS TEIKIMUI

Eil. Nr.	Charakteristika	Reikalavimai
1.	Paslaugų teikimo užtikrinimas	Virtualių tarnybinių stočių kopijavimo ir atstatymo paslauga visą jos teikimo laikotarpį turi apimti visą jai teikti reikalingą techninę ir programinę įrangą, apimant jos įsigijimą, įdiegimą bei priežiūrą, šios įrangos veikimui reikalingos infrastruktūros užtikrinimą, visas jai teikti reikalingas elektros energijos sąnaudas bei kitas su paslaugos teikimu susijusias sąnaudas.
2.	Paslaugos teikimo laikas	24x7
3.	Paslaugos pasiekiamumas	Ne blogiau kaip 99 % per mėnesį.
4.	Paslaugos kokybės reikalavimai	Reakcijos į incidentus laikas: ne ilgiau kaip 15 minučių. Incidentų išsprendimo laikas: ne ilgiau kaip 4 valandos. Reakcijos į užklausas ir keitimus laikas: ne ilgiau kaip 1 valanda. Užklausų ir keitimų išsprendimo laikas: ne ilgiau kaip 8 valandos.
5.	Atitikimo kokybės reikalavimams ataskaita	Tiekėjas turi pateikti paslaugų kokybės parametrų ataskaitą už praėjusį mėnesį, jeigu to reikalauja Pirkėjas. Ataskaitoje nurodomi šie duomenys: • Vidutinės incidentų reakcijos bei išsprendimo trukmės; • Visų incidentų sąrašas su nurodytais reakcijos bei išsprendimo laikais; • Mėnesio paslaugos pasiekiamumas.
6.	Sąsajos su kitomis paslaugomis	Tiekėjas turi pradėti teikti virtualių tarnybinių stočių kopijavimo ir atstatymo paslaugą pagal žemiau aprašytas charakteristikas ir techninius reikalavimus kartu su tarnybinių stočių perkėlimo paslauga.
7.	Funkcijos	• Virtualių tarnybinių stočių duomenų atsarginių kopijų sukūrimas; • Virtualių tarnybinių stočių duomenų atstatymas iš pasirinktos duomenų atsarginės kopijos.
8.	Rezervinių duomenų kopijų kūrimo ir atstatymo parametrai	• Virtualių tarnybinių stočių duomenų atsarginių kopijų sukūrimas turi būti atliekamas ne mažiau kaip 1 kartą per parą; • Turi būti saugomos ne mažiau kaip 7 paskutinių parų duomenų atsarginės kopijos; • Turi būti saugomos lokaliai duomenų centre greitam duomenų atstatymui.

9.	Papildomos nutolusių rezervinių duomenų kopijų laikymo sąlygos	• Virtualių tarnybinių stočių duomenų papildomų atsarginių kopijų sukūrimas turi būti atliekamas ne mažiau kaip 1 kartą per parą; • Turi būti saugomos ne mažiau kaip 7 paskutinių parų duomenų atsarginės kopijos; • Turi būti saugomos nutolusiame duomenų centre, aprašytoje dalyje Nr. 6 „Reikalavimai nutolusiam duomenų centrui“.
10.	Rezervinės kopijos funkcionalumo patikrinimas	Tiekėjas suteikia galimybę nemokamai atstatyti kiekvieno virtualaus serverio pasirinktą atsarginę kopiją 1 kartą per mėnesį, taip siekiant įsitikinti ar sukurtos atsarginės kopijos yra funkcionuojančios.
11.	Administravimo darbai, kuriuos atlieka Tiekėjas	• Tarnybinės stoties duomenų papildomos duomenų atsarginės kopijos sukūrimas; • Rezervinių duomenų kopijų sukūrimo plano atnaujinimas po atsarginių kopijų sukūrimo procedūrų pakeitimo; • Tarnybinių stočių duomenų atstatymo plano atnaujinimas po atsarginių kopijų atstatymo procedūrų pakeitimo.

10. REIKALAVIMAI VIRTUALIŲ TARNYBINIŲ STOČIŲ PERKĖLIMUI

Eil. Nr.	Charakteristika	Reikalavimai
1.	Paslaugų teikimo užtikrinimas	Virtualių tarnybinių stočių kopijavimo, perkėlimo ir atstatymo paslauga turi apimti visą jai teikti reikalingą techninę ir programinę įrangą, apimant jos įsigijimą, įdiegimą, šios įrangos veikimui reikalingos infrastruktūros užtikrinimą, visas jai teikti reikalingas elektros energijos sąnaudas bei kitas su paslaugos teikimu susijusias sąnaudas.
2.	Paslaugos teikimo laikas	Tiekėjas privalo perkelti virtualias tarnybines stotis iš Pirkėjo nurodytos infrastruktūros per techninėje specifikacijoje numatytą terminą.
3.	Paslaugos pasiekiamumas	Tiekėjas privalo užtikrinti paslaugų teikimo vientisumą perkėlimo metu, arba vykdyti perkėlimą nedarbo valandomis, suderintomis su Pirkėju.
4.	Paslaugos reikalavimai	Kiekvienos virtualios tarnybinės stoties perkėlimo scenarijus, privalo būti suderintas su Pirkėju. Tiekėjas perkelia virtualias tarnybines stotis iš esamo paslaugų tiekėjo į Tiekėjo naudojamą duomenų centro infrastruktūrą.
5.	Atitikimo kokybės reikalavimams	Tiekėjas privalo užtikrinti perkeltų tarnybinių stočių ir jose esančių paslaugų funkcionalumą.

11. REIKALAVIMAI VIRTUALIŲ TARNYBINIŲ STOČIŲ PRIEŽIŪRAI

11.1. Reikalavimai serverių stebėsenai:

Turi būti vykdoma nuolatinė serverių parametrų stebėseną. Kiekvienas parametras turi būti atnaujinamas ne rečiau kaip kas 5 minutes.

Stebėsenos parametrų reikšmės turi būti skirstomos bent į tris grupes:

- Normali reikšmė (angl. *normal*);
- Rizikinga reikšmė (angl. *warning*);
- Kritinė reikšmė (angl. *critical*).

Esant kritinei reikšmei, tačiau serverio veikimas nesutrikęs – Tiekėjas ne vėliau kaip per 24 valandas (o esant serverio neveikimo rizikai – nedelsiant) turi imtis veiksmų, kad pašalinti padidėjusią serverio neveikimo riziką.

Esant kritinei reikšmei ir serveris neveikia arba neveikia dalinai – fiksuojamas incidentas ir Tiekėjas turi imtis veiksmų, kad atstatyti normalų serverio darbą.

Esant rizikingai reikšmei – Tiekėjas turi vertinti konkrečią situaciją ir imtis veiksmų, siekiant sumažinti serverio neveikimo riziką.

Visais atvejais Tiekėjas turi siekti užtikrinti, kad visų stebimų parametrų reikšmė būtų „Normali“.

11.2. Bendri reikalavimai taikomi visų serverių (Linux ir Windows) priežiūrai:

Eil. Nr.	Charakteristika	Reikalavimai
1.	Serverių parametrų nuolatinė stebėseną	Tiekėjas pasirenka, kuriuos serverių parametrus stebėti, kad būtų užtikrintas nenutrūkstamas serverių darbas, tačiau būtinai turi būti stebimi žemiau nurodyti parametrai: • CPU apkrovimo stebėseną; • RAM laisvos atminties stebėseną; • Disko laisvos vietos stebėseną (stebimos atskiros disko particijos); • Disko I/O apkrovimas; • PING atsakymo greitis; • Procesų, veikiančių serveryje, kiekis; • SWAP segmento dydis.
2.	Windows OS naujinimas	Visi atnaujinimai turi būti atliekami kaip planiniai darbai. Turi būti diegiami oficialūs Microsoft išleisti Windows OS atnaujinimai: • kuo skubiau turi būti diegiami kritiniai saugumo pataisymai; • ne vėliau kaip per 14 kalendorinių dienų turi būti įdiegiami kiti atnaujinimai, darantys įtaką konkrečiam serverio darbui. Prieš diegiant atnaujinimus, turi būti sukurama virtualios mašinos atsarginė kopija (angl. <i>snapshot</i>). Po atnaujinimų diegimo atliekamas minimalus serverio veikimo testavimas ir tik po sėkmingo testavimo gali būti ištrinama šio serverio atsarginė kopija.

3.	Linux OS naujinimas	Visi atnaujinimai turi būti atliekami kaip planiniai darbai. Turi būti diegiami tik kritiniai Linux programinės įrangos atnaujinimai. Visi kiti Linux atnaujinimai turi būti derinami su Pirkėju.
4.	Windows OS licencijų stebėseną	Tiekėjas turi užtikrinti, kad būtų nepažeidžiamos programinės įrangos licencijavimo sąlygos. Apie bet kokią galimą licencijavimo taisyklių pažeidimą Tiekėjas turi informuoti Pirkėją (pvz. naudojamų Microsoft RDC licencijų kiekis).
5.	Serverių valdymas	Pirkėjo nurodymu atliekami šie darbai su virtualiais serveriais: • Naujo serverio parengimas pagal Pirkėjo suformuluotą poreikį; • Serverio panaikinimas; • Serverio išjungimas ar įjungimas; • Serverio konfigūracijos keitimas (įskaitant serverio programinės įrangos įdiegimą, išdiegimą ar konfigūravimą).
6.	Tarpininkavimas	Tarpininkavimas tarp Pirkėjo ir duomenų centro paslaugų Tiekėjo dėl duomenų centro paslaugų teikimo, incidentų metu.

12. REIKALAVIMAI VIETINIO KOMPIUTERINIO TINKLO PRIEŽIŪRAI

Šiuo metu Pirkėjui nuosavybės teise priklauso bei veikia ši techninė tinklo įranga:

- Mikrotik RB3011 – pagrindinis maršrutizatorius, užtikrinantis interneto ryšį ir IPSEC šifruotą L2 sujungimą su duomenų centru;
- Mikrotik cAP ac (2 vnt.) – Wi-Fi maršrutizatorius.
- Aruba 6100 24G CL4 4SFP+ Swich – tinklo komutatorius.

Eil. Nr.	Charakteristika	Reikalavimai
1.	Laidinis LAN	Visose KDV, kur yra techninės galimybės, turi veikti laidinis LAN ryšys su PoE palaikymu, ne prastesnių savybių kaip numatyta IEEE 802.3af standarte bei palaikanti 10/100/1000 Gbps full duplex greitaveiką.
2.	Wi-Fi įrenginiai	Užsakovo patalpose turi veikti ne mažiau kaip du Wi-Fi įrenginiai veikiantys dviejų dažnių diapazone (2.4 GHz ir 5 GHz)
3.	Wi-Fi saugumas	Visi Wi-Fi prisijungimai turi būti atliekami naudojant ne žemesnio saugumo (šifravimo) lygį kaip WPA2.
4.	Wi-Fi vietinis tinklas KDV	Turi būti sukurtas atskiras potinklis skirtas KDV. Prisijungus šiuo būdu, KDV turi būti pasiekiami visi resursai (internetas ir duomenų centro serveriai) kaip ir jungiant KDV prie LAN naudojant kabelį. Turi būti galimybė jungtis tiek prie 2.4 GHz, tiek prie 5 GHz tinklo.

5.	Wi-Fi vietinis tinklas specifiniams įrenginiams	Turi būti sukurta atskira galimybė prie Wi-Fi vietinio tinklo jungtis įrenginiams naudojant slaptažodį. Tam turi būti sukurtas atskiras paslėptas tinklas (angl. <i>hidden SID</i>). Prisijungus šiuo būdu, įrenginyje turi būti pasiekiami visi resursai (internetas ir duomenų centro serveriai), kaip ir jungiantis prie LAN naudojant kabelį.
6.	Wi-Fi internetas svečiams	Turi būti sukurtas atskiras potinklis svečiams, kuris būtų atskirtas nuo įmonės vietinio tinklo ir duomenų centro. Prisijungus prie šio Wi-Fi tinklo, turi būti pasiekiami tik vieši interneto resursai. Prie šio tinklo prisijungimas vykdomas suvedant slaptažodį, kuris Pirkėjo nurodymu gali būti keičiamas, bet ne dažniau kaip 4 kartus per metus. Turi būti galimybė jungtis tiek prie 2.4 GHz, tiek prie 5 GHz tinklo. Wi-Fi tinkle turi būti palaikomi bent šie svečių naudojami standartiniai įrenginiai su operacinėmis sistemomis: Android OS, iOS, Windows.
7.	Wi-Fi tinklo veikimas kai įrenginys nešiojamas	Abu veikiantys Wi-Fi įrenginiai turi turėti tuos pačius tinklo pavadinimus (angl. <i>SID</i>). Nešiojant prie Wi-Fi prisijungusį kompiuterį ar kitą mob. įrenginį, automatiškai turi būti parenkamas tinkamas Wi-Fi įrenginys nenutrūkstant esamam tinklui (pvz. naudojant WDS, Mikrotik Mesh ar kitą alternatyvią technologiją).
8.	IP adresai	IP adresai turi būti priskiriami automatiškai, su galimybe konkrečiam MAC adresui nustatyti, kad būtų visada priskiriamas tas pats IP (pvz. spausdintuvams).
9.	Techninės įrangos pakeitimas alternatyvia	Pirkėjo patalpose (biure) veikianti techninė įranga, Tiekėjo kaštais gali būti pakeista nauja alternatyvia, ne prastesne technine įranga, užtikrinant esamos Mikrotik įrangos funkcionalumą, įskaitant aparatinį IPSEC palaikymą L2 ryšiui su duomenų centru.
10.	Techninės įrangos veikimo užtikrinimas	Tiekėjas turi užtikrinti techninės įrangos nuolatinį veikimą. Gedimo atveju turi kuo greičiau pakeisti ar sutaisyti įrangą, arba rasti alternatyvų laikiną sprendimą (pvz.: pagrindinio maršrutizatoriaus gedimo atveju, jis laikinai gali būti pakeičiamas koku nors standartiniu maršrutizatoriumi ir nurodant vartotojams prie duomenų centro jungtis naudojant VPN).
11.	Užsakovo sujungimas su DC	Užtikrinti šifruotą IPSEC VPN ir L2 sujungimą tarp duomenų centre veikiančio virtualaus maršrutizatoriaus ir KDV. L2 IPSEC sujungimas turi užtikrinti saugų serverių resursų pasiekiamumą iš KDV. Pats L2 ryšys tarp duomenų centro ir Pirkėjo biuro patalpose esančių maršrutizatorių nėra Tiekėjo atsakomybė.

13. REIKALAVIMAI VIRTUALAUS SERVERIO SU MARŠRUTIZATORIAUS PROGRAMINE ĮRANGA IR UGNIASIENĖS PRIEŽIŪRAI

Šiuo metu virtualiame serveryje veikia FortiGate VM 64 v7.2 programinė įranga. FortiGate programinė ir techninė įranga, Tiekėjo kaštais gali būti pakeista alternatyvia, ne prastesnių parametrų nauja įranga, užtikrinat esamą FortiGate įrangos funkcionalumą.

Eil. Nr.	Charakteristika	Reikalavimas
1.	DOS atakų apsauga	Turi būti stebimas prisijungimų skaičius iš vieno IP ir pasiekus kritinę ribą – IP turi būti blokuojamas.
2.	VPN	Turi būti galimybė Pirkėjo darbuotojams, naudojant šifruotą SSL VPN, prisijungti prie visų duomenų centre esančių resursų, prie kurių jie turi prieigos teises. Prisijungimo autorizavimas turi būti vykdomas naudojant SSO (angl. <i>Single Sign-On</i>) per Entra AD. VPN sprendimas turi užtikrinti aukštą saugumo lygį, įskaitant šifravimą, autentifikaciją ir apsaugą nuo neteisėto prisijungimo.
3.	Sujungimas tarp duomenų centro ir Pirkėjo biuro	Turi būti užtikrinamas IPSEC VPN ir koduotas L2 sujungimas tarp duomenų centro ir Užsakovo biuro (Pirkėjo biure veikia nuosavas Mikrotik RB3011 maršrutizatorius bei Mikrotik cAP Wi-Fi įrenginiai). Visos Pirkėjo KDV turi turėti prieigą prie visų duomenų centre esančių resursų, prie kurių jos turi prieigos teises.
4.	Pasiekiamumas iš išorės	Serverių pasiekiamumas iš išorės (interneto) turi būti tik toks, kokio būtinai reikia serverio teikiamai funkcijai užtikrinti.
5.	Srautų ribojimas	Pagal Pirkėjo poreikius gali būti ribojamas perduodamų duomenų greitis. Vidiniai duomenų srautai ir VPN prisijungimo metu perduodamų duomenų greitis neturi būti ribojamas.
6.	Ugniasienės atnaujinimas	Ugniasienės programinė įranga turi būti reguliariai atnaujinama, kai tik pasirodo gamintojo pateikti saugumo ar funkcionalumo atnaujinimai. Prieš diegiant atnaujinimus turi būti sukurama virtualios mašinos atsarginė kopija (angl. <i>snapshot</i>). Po atnaujinimų diegimo atliekamas minimalus ugniasienės veikimo testavimas ir tik po sėkmingo testavimo, gali būti ištrinama šios virtualios mašinos atsarginė kopija.
7.	Tinklo segmentavimas	Turi būti užtikrintas aiškus tinklo segmentavimas tarp šių potinklų: • LAN – vidinis tinklas, skirtas darbuotojų darbo vietoms ir vidinėms paslaugoms. • DMZ-PROD – demilitarizuota zona, skirta produkcinėms paslaugoms, pasiekiamoms iš išorės. • DMZ-TEST – demilitarizuota zona, skirta testavimo aplinkai. Segmentavimas turi būti įgyvendintas naudojant ugniasienės

		taisykles ir tinklo politiką, užtikrinant saugų ir kontroliuojamą srautų judėjimą tarp segmentų. Turi būti galimybė taikyti skirtingas saugumo politikas kiekvienam segmentui.
8.	Konfigūravimas	Pagal Pirkėjo poreikius turi būti atliekami kiti ugniasienės konfigūravimo darbai.
9.	Priežiūra	Tiekėjas savo kompetencijos ribose Pirkėjui teikia rekomendacijas dėl ugniasienės konfigūracijos optimizavimo, saugumo didinimo, saugumo spragų taisymo, papildomų sprendimų įdiegimo.

14. PRIEŽIŪROS PASLAUGŲ KOKYBINIAI PARAMETRAI

Paslaugos pavadinimas	Paslaugos priežiūros valandos	Reakcijos laikas į užklausas	Reakcijos laikas į incidentus	Užklausų sprendimo laikas	Incidentų sprendimo laikas
Virtualių serverių priežiūra	Sistemų parametrų stebėsena, Pirkėjo pateikiamos užklausos ir incidentai darbo dienomis 8:00 – 17:00 val.	4 val.	1 val.	8 val.	4 val.
Tinko priežiūra	Tinklo parametrų stebėsena, Pirkėjo pateikiamos užklausos ir incidentai darbo dienomis 8:00 – 17:00 val.	4 val.	1 val.	8 val.	4 val.

Incidentų ir (ar) užklausų skaičius neribojamas.

Reakcijos laikas - laiko tarpas nuo Pirkėjo pranešimo apie incidentą ar užklausos gavimo (Pirkėjas incidentus ir užklausas registruoja telefonu arba el. paštu) iki incidento ar užklausos pradėjimo spręsti konkrečiam Tiekėjo specialistui.

Sprendimo laikas – laiko tarpas nuo Pirkėjo užregistruoto incidento ar užklausos pradėjimo spręsti konkrečiam Tiekėjo specialistui iki šio užregistruoto incidento ar užklausos išsprendimo.

15. REIKALAVIMAI DUOMENŲ SAUGAI IR INFORMACIJOS KONFIDENCIALUMUI:

15.1. Siekiant užtikrinti Tiekėjo duomenų centro veikimo patikimumą, nepertraukiamumą ir elektroninės informacijos saugą, turi būti įgyvendinti infrastruktūros veikimo patikimumo, nepertraukiamumo, duomenų atsarginio kopijavimo, saugos ir veiklos tęstinumo užtikrinimo reikalavimai, nustatyti:

- Bendrajame duomenų apsaugos reglamente, įsigaliojusiame 2018 m. gegužės 25 d.

- Techninės specifikacijos priedėlis Nr. 1 „Minimalūs informacijos saugos reikalavimai“.

Teisės aktuose nustatyti šie pagrindiniai reikalavimai, susiję su Paslaugos atlikimu:

15.1.1. prieiga prie Pirkėjui pateikiamos infrastruktūros gali būti suteikiama tik tam asmeniui, kuriam prieiga reikalinga priskirtiems darbams atlikti;

15.1.2. kiekvienas infrastruktūros naudotojas gaunamų paslaugų apimtyje turi būti unikaliai identifikuojamas ir autentifikuojamas. Naudotojų autentifikavimas, autorizavimas ir naudotojų valdymas turi būti realizuotas vaidmenų pagrindu;

15.1.3. turi būti užtikrinti infrastruktūros naudotojų slaptažodžių saugumo reikalavimai (slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių ir kt.);

15.1.4. teikiant Paslaugą Pirkėjui, turi būti naudojama tik legali programinė įranga;

15.1.5. turi būti užtikrinamas patalpų, kuriose yra Pirkėjui pateikiama infrastruktūra, saugumas (apriojamas neįgaliotų asmenų patekimas į atitinkamas patalpas ir kt.);

15.1.6. patalpose, kuriose yra Pirkėjui pateikiama infrastruktūra, turi būti oro kondicionavimo ir drėgmės kontrolės įranga, įrengti gaisro ir įsilaužimo davikliai;

15.1.7. duomenų centro įranga turi turėti įtampos filtrą ir rezervinį maitinimo šaltinį.

15.2. 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.

15.3. Tiekėjas privalo užtikrinti, kad duomenų laikmenos su Pirkėjo informacija nebus perduodamos tretiesiems asmenims.

15.4. Tiekėjas privalo užtikrinti, kad Pirkėjo informacija nebus nukopijuota ir (ar) perduodama tretiesiems asmenims.

15.5. Paslaugų teikimo metu tiekėjas privalo užtikrinti apsaugą nuo įsilaužimų, duomenų vagysčių, kibernetinių atakų.

15.6. Tiekėjas privalo informuoti Pirkėją apie duomenų centro infrastruktūroje įvykusius kibernetinius incidentus ir jų poveikį.

15.7. Tiekėjas privalo užtikrinti apsaugą nuo kenksmingos programinės įrangos. Taip pat Tiekėjas turi užtikrinti jo duomenų centre Pirkėjo patalpintų resursų apsaugą, naudojant tinklo ugniasienes.

15.8. Tiekėjas privalo užtikrinti, kad Pirkėjui skirti resursai (virtualios tarnybinės stotys, virtualus tinklas ir t.t.) bus atskirti nuo kitiems tiekėjo klientams skirtų resursų.

15.9. Elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijas neteisėtai atkurti elektroninę informaciją.