2025 m. d.

paslaugų viešojo pirkimo–pardavimo sutarties Nr. 1 priedas

**TECHNINĖ SPECIFIKACIJA**

|  |
| --- |
| **Reikalavimai susiję su nacionaliniu saugumu** |
| **Pirkimo objektui taikomi Lietuvos Respublikos viešųjų pirkimų įstatymo 37 str. 8 dalies ir 9 dalies reikalavimai susiję su nacionaliniu saugumu:**  **1. Pirkimo objektui taikomi Lietuvos Respublikos viešųjų pirkimų įstatymo 37 str. 8 dalies reikalavimai susiję su nacionaliniu saugumu.** Perkančioji organizacija, veikianti srityse, kurios laikomos nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi, ar valdanti ypatingos svarbos informacinę infrastruktūrą, reikalauja, kad Paslaugų teikėjo siūlomos paslaugos nekeltų grėsmės nacionaliniam saugumui, kai sandorio pagrindu susidarytų aplinkybės, nurodytos Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo 13 straipsnio 4 dalies 1 punkte. Laikoma, kad Paslaugų teikėjo siūlomos paslaugos kelia grėsmę nacionaliniam saugumui, kai Lietuvos Respublikos Vyriausybė yra priėmusi sprendimą, patvirtinantį, kad ketinamas sudaryti sandoris neatitinka nacionalinio saugumo interesų vadovaujantis Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymu, ir Paslaugų teikėjo pasiūlymas atmetamas.  **2. Pirkimo objektui taikomi Lietuvos Respublikos viešųjų pirkimų įstatymo 37 str. 9 dalies reikalavimai susiję su nacionaliniu saugumu\*.** Paslaugų teikėjas privalo įrodyti, kad siūlomos paslaugos nekelia grėsmės nacionaliniam saugumui, nėra toliau nurodytų aplinkybių - paslaugų teikimas būtų vykdomas iš VPĮ 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų.  **Perkančioji organizacija pasiūlymo atitikčiai LR viešųjų pirkimų įstatymo 37 straipsnio 9 dalies reikalavimams patvirtinti iš Paslaugų teikėjo reikalauja KARTU SU PASIŪLYMU** **PATEIKTI užpildytą pirkimo dokumentą „Nacionalinio saugumo reikalavimų atitikties deklaracija“ (8 IA PD ATITIKTIES DEKLARACIJA), o iš ekonomiškai naudingiausią pasiūlymą pateikusio Paslaugų teikėjo reikalaus pateikti (kartu su pasiūlymu šių dokumentų Paslaugų teikėjas pateikti neturi) – vieną ar kelis šiuos dokumentus\*\*: juridinio asmens vadovo patvirtintą juridinio asmens steigimo dokumentų kopiją, Juridinių asmenų registro išplėstinį išrašą su istorija, Juridinių asmenų dalyvių informacinės sistemos išrašą, asmens tapatybę patvirtinančio dokumento (tapatybės kortelės ar paso) kopiją, leidimo verstis atitinkama ūkine veikla patvirtinančio dokumento (pavyzdžiui, verslo liudijimo, individualios veiklos pažymėjimo ir pan.) kopiją, pažymą apie deklaruotą gyvenamąją vietą arba atitinkamus valstybės narės ar trečiosios šalies dokumentus, ar kitus perkančiajai organizacijai priimtinus dokumentus.**  **Pastabos:**  \*Jeigu prekių gamintojas ar Paslaugų teikėjas ar jį kontroliuojantis asmuo yra nacionaliniam saugumui užtikrinti svarbi įmonė, valstybės įmonė, savivaldybės įmonė, taip pat valstybės valdoma bendrovė ir jų dukterinės bendrovės, išvardytos Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme, šiems subjektams aukščiau nurodytas reikalavimas (VPĮ 37 straipsnio 9 dalis) yra netaikomas.  \*\*Dokumentai, kuriuose nenurodytas jų galiojimo terminas, turi būti išduoti ar atspausdinti iš informacinės sistemos ne anksčiau kaip likus 3 mėnesiams iki tos dienos, kurią perkančiosios organizacijos prašymu Paslaugų teikėjas turi pateikti dokumentus. |

Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – IRD, Klientas, perkančioji organizacija) yra Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir informacinių sistemų tvarkytojas ir užtikrina techninės ir programinės įrangos nepertraukiamą veikimą bei saugą. Šiose pirkimo sąlygose pirkimo objektui apibūdinti galimai nurodyti konkretūs techniniai parametrai, technologijos, procesai, gamintojai ar prekės ženklai, standartai, tipai yra tik informacinio pobūdžio. Paslaugų teikėjas gali siūlyti ir lygiaverčius produktus, tačiau siūlomų analogiškų arba lygiaverčių produktų parametrai negali būti prastesni nei reikalaujami. Siūlomų „lygiaverčių“ prekių lygiavertiškumą turi įrodyti Paslaugų teikėjas.

Pirkimo objektui taikomas Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo, patvirtinto Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 „Dėl Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo patvirtinimo“, 4.4.3 papunktis.

**1. Registrų ir informacinių sistemų techninę ir sisteminę programinę įrangą (RISTSPĮ) sudarančių komponentŲ sąrašas**

1.1. Centrinė duomenų bazė (CDB), veikianti „Oracle Database 10g“ ir „Oracle Database 12“, taip pat „Real Application Cluster“ pagrindu, turinti sąsajas su kitomis vidinėmis ir išorinėmis informacinėmis sistemomis.

1.2. Produkcinės ir testavimo duomenų bazės, veikiančios „Oracle Database 10g“, „Oracle Database 12c“ ir „Oracle Database 19c“ pagrindu, Microsoft SQL server pagrindu.

1.3. Taikomųjų programų valdymo sistemos, veikiančios „Oracle Application Server 10g, Oracle Weblogic 12 v. Tomcat ir Java pagrindu.

1.4. Taikomųjų programų valdymo sistemos, veikiančios „Oracle Enterprise Service Bus.1.5. Didelio našumo skaičiavimo telkinys, veikiantis Windows Server 2012/2019 Datacenter, VMware pagrindu.

1.5. Integracinė platforma, veikianti „WebMethods“ ir „Oracle Servis Bus“ pagrindu.

1.6. Rezervinio duomenų kopijavimo sistema, veikianti „IBM Tivoli Storage Manager“, HPE StoreOnce 5100 System ir „Veeam Backup & Replication” pagrindu.

1.7. Elektroninio pašto sistema, veikianti „Microsoft Exchange 2019“, „Windows Server“ ir “Linux” pagrindu.

1.8. Centralizuoto valdymo įranga, veikianti „IBM Tivoli“ ir „Active Directory“ pagrindu.

1.9. Internetinės svetainės, veikiančios „Windows Server“ ir “Linux” pagrindu.

1.10. Atviro kodo programinės įrangos sistemos (SVN, Redmine, Nextcloud, Nagios, Postfix, RoundCube, Dovecot, PolicyD, AWStats ir kt.).

1.11. Tarnybinių stočių virtualizavimo sprendimai, VMware vSphere.

1.12. Tarnybinės stotys, kuriose įdiegtos aukščiau išvardintos sistemos.

1.13. Tarnybinių stočių SAN tinklo ir duomenų saugyklų virtualizacijos įrenginiai.

1.14. Magnetinių juostų biblioteka ir duomenų saugyklos, naudojamos rezerviniam kopijavimui.

1.15. Tarnybinių stočių duomenų perdavimo SAN ir LAN tinklai bei aktyvinė duomenų perdavimo įranga.

**2. RISTSPĮ techninės įrangos ir operacinių sistemų sąrašas**

* 1. Tarnybinės stotys IBM x3500 M4, IBM x3850, operacinė sistema Redhat Linux.
  2. Tarnybinės stotys IBM x336, IBM Hardware Management Console (HMC).
  3. Tarnybinė stotis IBM x3650 M4, IBM Infosphere Guardium Database Activity Monitoring Suite.
  4. VMware infrastruktūros serverių talpyklos HPE Synergy 12000 Frame, tarnybinės stotys HPE Synergy 480 Gen10, HPE Synergy 660 Gen10.
  5. Virtualūs serveriai (produkciniai ir testiniai), veikiantys VMware platformoje, operacinės sistemos Microsoft Windows Server (2008, 2012, 2016, 2019), Linux (CentOS, Debian, Oracle, Redhat, Ubuntu) ir kt.
  6. Duomenų saugyklos HPE 3PAR StoreServ 8400, IBM FlashSystem 5100, IBM Flash System 5035.
  7. Rezervinio kopijavimo (*backup*) įranga: duomenų saugyklos HPE StoreOnce 5100, juostų biblioteka IBM TS4300.
  8. „Smėlio dėžė“ Fortinet Fortisandbox 1000D.
  9. El. pašto apsaugos įranga Fortinet Fortimail 400F.
  10. Aplikacijų ugniasienės F5 BIG-IP i4000 Series.
  11. Ugniasienės Fortinet FortiGate 1101E, FortiGate 1801F.
  12. Tinklo infrastuktūra: LAN komutatoriai, Cisco Catalyst (2960G, 3560G, 3650), Cisco Nexus (31108PCV), Cisco (9300, 9500).
  13. Tinklo infrastruktūra: SAN komutatoriai IBM 2498-F48, Brocade.
  14. SMS maršrutizatoriai TELTONIKA TRB140.

1. **REGISTRŲ IR INFORMACINIŲ SISTEMŲ TECHNINĖS IR SISTEMINĖS PROGRAMINĖS ĮRANGOS PRIEŽIŪROS APIMTIES REIKALAVIMAI**
   1. **RISTSPĮ kritinių sutrikimų šalinimas**

3.1.1. Kritinio sutrikimo šalinimo darbai apima:

* + kritinio sutrikimo priežasčių diagnostika;
  + sutrikimo šalinimo būdo parinkimas ir suderinimas su užsakovo įgaliotais specialistais;
  + pilnas sutrikusio RISTSPĮ komponento veikimo atstatymas;
  + prarastų ar sugadintų duomenų atstatymas, jeigu yra toks poreikis ir techninė galimybė;
* prevencinių priemonių įgyvendinimas, kad sutrikimas nepasikartotų.

3.1.2. Kritinių sutrikimų šalinimo paslaugos turi būti teikiamos 24 valandas per parą, 7 dienas per savaitę.

* 1. **RISTSPĮ įrangos nekritinių sutrikimų šalinimas, profilaktinė priežiūra, veikimo optimizavimas, funkcionalumo vystymas**

3.2.1 Nekritinių sutrikimų šalinimo, profilaktinės priežiūros, veikimo optimizavimo, funkcionalumo vystymo darbai apima:

* + nekritinių sutrikimų priežasčių diagnostika ir RISTSPĮ įrangos įprasto veikimo atkūrimas;
  + programinės įrangos klaidų ir saugumo spragų diagnozavimas, pataisymų parengimas, testavimas ir diegimas;
  + RISTSPĮ sutrikimų prevencijos rekomendacijų teikimas ir jų įgyvendinimas;
  + RISTSPĮ saugumo pagerinimo rekomendacijų teikimas ir jų įgyvendinimas;
  + RISTSPĮ klaidų žurnalų analizė ir rekomendacijų, kaip išvengti galimų sutrikimų, teikimas;
  + galimų sutrikimų dėl techninių resursų trūkumo prognozė;
  + naudojamų techninių ir programinės įrangos resursų optimizavimas RISTSPĮ našumui ir saugumui užtikrinti;
  + sisteminės programinės įrangos atnaujinimų ir pataisymų diegimas;
* papildomo funkcionalumo detalios specifikacijos rengimas ir derinimas;
* papildomo funkcionalumo analizės, projektavo, kūrimo, testavimo ir diegimo darbai;
* techninės dokumentacijos aktualizavimas;
* administratorių konsultavimas RISTSPĮ eksploatacijos klausimais.

3.2.2 Užduoties derinimas ir įgyvendinimas vykdomas darbo valandomis pagal perkančiosios organizacijos ir Paslaugų teikėjo suderintą grafiką.

1. **REGISTRŲ IR INFORMACINIŲ SISTEMŲ TECHNINĖS IR SISTEMINĖS PROGRAMINĖS ĮRANGOS PRIEŽIŪROS DARBŲ PROCEDŪRA**

4.1. RISTSPĮ techninės priežiūros paslaugos teikiamos pagal perkančiosios organizacijos poreikį per visą sutarties galiojimo laikotarpį.

4.2. Vykdant IT infrastruktūros techninę priežiūrą Paslaugų teikėjo ekspertai su perkančiosios organizacijos atstovais turi komunikuoti lietuvių kalba arba Paslaugų teikėjas turi užtikrinti vertimą į lietuvių kalbą.

4.3. Perkančiosios organizacijos kreipiniai skirstomi į dvi kategorijas, aprašytas 1 lentelėje „Kreipinių kategorijos“.

1 lentelė. Kreipinių kategorijos

|  |  |  |  |
| --- | --- | --- | --- |
| **Eil. Nr.** | **Kreipinio kategorija** | **Reakcijos laikas \*** | **Sprendimo laikas \*** |
| 1 | **I prioritetas.** RISTSPĮ techninės ir programinės įrangos funkcionalumo kritiniai sutrikimai, kai perkančiosios organizacijos pagrįsta nuomone, naudotojai negali tęsti darbo (techninės specifikacijos 3.1. punktas). | 1 val. | ne ilgiau kaip 8 valandos |
| 2 | **II prioritetas.** RISTSPĮ nekritinių sutrikimų šalinimas, profilaktinė priežiūra, veikimo optimizavimas, funkcionalumo vystymas (techninės specifikacijos 3.2 punktas) | 1 darbo diena. | Problemos sprendimas vykdomas darbo valandomis pagal perkančiosios organizacijos ir Paslaugų teikėjo suderintą terminą |

***\*Reakcijos laikas*** *– tai laikotarpis nuo kreipinio registravimo laiko iki laiko, kai kreipinyje nurodytas perkančiosios organizacijos prašymas pradedamas vykdyti.*

***\*Sprendimo laikas*** *– tai laikotarpis nuo reakcijos laiko pradžios iki kreipinyje nurodytų klausimų išsprendimo – visiško paslaugų funkcionalumo pagal paraiškoje nurodytus parametrus atkūrimo, arba perkančiosios organizacijos kreipinyje nurodyto darbo atlikimo.*

4.4. I prioriteto kreipinių valdymo tvarka:

4.4.1. Kreipiniai kritinių sutrikimų šalinimo paslaugoms teikiami individualiai ir apskaitomi Perkančiosios organizacijos Informacinių technologijų ir telekomunikacijų paslaugų valdymo posistemėje (ITT pagalbos sistema).

4.4.2. Perkančiosios organizacijos įgaliotiems asmenims ITT pagalbos sistemoje užregistravus kritinį sutrikimą, iš ITT pagalbos sistemos kreipiniai dėl incidento elektroniniu paštu siunčiami į Paslaugų teikėjo paslaugų tarnybos sistemą.

4.4.3. Apie užfiksuotą kritinį sutrikimą telefonu pranešama Paslaugų teikėjo įgaliotiems asmenims.

4.4.4. Apie kritinio sutrikimo sprendimo būseną Paslaugų teikėjas turi informuoti Perkančiąją organizaciją el. paštu ittpagalba@vrm.lt, laukelyje „Tema“ (angl. Subject) nurodydamas tą patį kreipinio numerį, kuris buvo gautas iš Perkančiosios organizacijos.

4.5. II prioriteto kreipinių valdymo tvarka:

4.5.1. Kreipiniai nekritinių sutrikimų šalinimo, profilaktinės priežiūros, veikimo optimizavimo, funkcionalumo vystymo paslaugoms yra individualiai apskaitomi perkančiosios organizacijos pavedimų sistemoje.

4.5.2. Perkančioji organizacija užregistruoja paslaugų poreikį https://pavedimai.vrm.lt sistemoje ir apie šį poreikį informuoja Paslaugų teikėjo paskirtus atstovus.

4.5.3. Paslaugų teikėjas įvertina paslaugų poreikio įgyvendinimo darbo laiko sąnaudas bei įgyvendinimo terminus ir pateikia Perkančiajai organizacijai savo vertinimus.

4.5.4. Perkančiajai organizacijai patvirtinus planuojamas laiko sąnaudas ir terminus, Paslaugų teikėjas vykdo kreipinyje suderintas veiklas.

4.5.5. Įvykdęs kreipinyje užsakytus darbus, Paslaugų teikėjas pateikia atliktų darbų ataskaitą, kurioje nurodo faktines darbo laiko sąnaudas.

4.6. Funkcionalumo vystymo paslaugoms Paslaugų teikėjas suteikia 12 mėnesių garantinį laikotarpį nuo šių paslaugų perdavimo-priėmimo akto pasirašymo dienos, kurio metu nemokamai šalina sutrikimus 4.3 p. nustatytais terminais.

**5. TEISĖS AKTAI**

5.1. Teisės aktai, kuriais turi vadovautis Paslaugų teikėjas:

5.1.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

5.1.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

5.1.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

5.1.4. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

5.1.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl bendrųjų elektroninės informacijos saugos reikalavimų aprašo, saugos dokumentų turinio gairių aprašo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

5.1.6. Valstybinės duomenų apsaugos inspekcijos metodiniai dokumentai dėl duomenų saugumo priemonių ir rizikos įvertinimo, pritaikytosios ir standartizuotosios duomenų apsaugos informacinės sistemos gyvavimo cikle ir kiti metodiniai dokumentai ir rekomendacijos;

5.1.7. Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos metodiniai dokumentai ir rekomendacijos;

5.1.8. Kiti susiję teisės aktai ir jų redakcijos.

5.2. Paslaugų teikėjas privalo vadovautis ne tik aukščiau išvardintais, bet ir visais kitais su Sutarties įgyvendinimu susijusiais teisės aktais, taip pat jų naujausiais pakeitimais ir papildymais. Paslaugų teikėjas turi vadovautis vykdymo metu naujai priimtais teisės aktai, jeigu jie susiję su Sutarties įgyvendinimu.

**6. KITI REIKALAVIMAI, SUSIJĘ SU KIBERNETINIU SAUGUMU**

6.1. Paslaugų teikėjas privalo atlikti šiuos veiksmus ir pranešti apie kibernetinį incidentą, įvykusį jo tinklų ir informacinių sistemų infrastruktūroje, perkančiajai organizacijai šiais terminais ir nurodyti tokią informaciją:

6.1.1. nedelsiant, bet ne vėliau kaip per 24 valandas nuo sužinojimo apie didelį kibernetinį incidentą momento – pateikti ankstyvąjį perspėjimą, kuriame pagal galimybes nurodoma, ar didelį kibernetinį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai ir ar jis galėtų daryti tarpvalstybinį poveikį;

6.1.2. nedelsiant, bet ne vėliau kaip per 72 valandas nuo sužinojimo apie kitą kibernetinį incidentą momento – pateikti ankstyvąjį perspėjimą apie kitą kibernetinį incidentą, kuriame pagal galimybes nurodoma ar kibernetinį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai ir ar jis galėtų daryti poveikį perkančiosios organizacijos tinklams ir informacinėms sistemoms;

6.1.3. ne vėliau kaip per vieną mėnesį nuo 6.1.1 ar 6.1.2 papunktyje nurodyto pranešimo apie kibernetinį incidentą pateikimo dienos – pateikti galutinę ataskaitą, kurioje pateikiama informacija, nurodyta ši informacija pagal Kibernetinio saugumo įstatymo 18 straipsnio 4 dalies 4 punktą.

6.2. Perkančioji organizacija arba jos įgalioti paslaugų teikėjai turi teisę atlikti Paslaugų teikėjo atitikties Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, (toliau – Aprašas), reikalavimams auditą (įskaitant neplaninį), o ir Paslaugų teikėjas turi pareigą sudaryti sąlygas tokiam auditui atlikti sutarties vykdymo laikotarpiu ar įvykus dideliam incidentui.

6.3. Paslaugų teikėjas visą sutarties vykdymo laikotarpį privalo ne rečiau kaip kartą per metus, įvykus esminiams kibernetinio saugumo subjekto organizaciniams ar kitiems reikšmingiems pokyčiams, taip pat įvykus dideliam kibernetiniam incidentui atlikti savo valdomų tinklų ir informacinių sistemų rizikos vertinimą. Taip pat, reguliariai, ne rečiau kaip kartą per metus, įvertinti savo atitiktį Kibernetinio saugumo įstatymui, Aprašo ir Paslaugų teikėjo patvirtintiems kibernetinio saugumo politikos dokumentuose nustatytiems reikalavimams. Paslaugų teikėjas įsipareigoja perkančiajai organizacijai pareikalavus pateikti visą reikalingą informaciją, dokumentus, reikalingus įsitikinti, kad Paslaugų teikėjas atlieka rizikos ir atitikties vertinimus.

6.4. Paslaugų teikėjas įsipareigoja užtikrinti jo tinklų ir informacinės sistemų spragų, keliančių riziką perkančiosios organizacijos tinklams ir informacinėms sistemoms, valdymą.

6.5. Paslaugų teikėjas įsipareigoja užtikrinti, kad jo patalpos, įranga, tinklai ir informacinių sistemų priežiūra, informacijos perdavimas tinklais atitinka Aprašo reikalavimus.

6.6. Paslaugų teikėjui fizinė prieiga prie perkančiosios organizacijos tinklų, kitos techninės infrastruktūros ir informacinių sistemų nėra suteikiama. Paslaugų teikėjui suteikiama loginė prieiga per perkančiosios organizacijos saugų VPN sprendimą prie kūrimo ar testavimo aplinkų. Atskiru perkančiosios organizacijos sprendimu (pvz. sprendžiant kritinius incidentus), laikina loginė prieiga gali būti suteikta prie darbinių aplinkų. Loginė prieiga suteikiama prie perkančiosios organizacijos kontroliuojamo nuotolinio darbalaukio serverio, kuriame visi Paslaugų teikėjo veiksmai yra fiksuojami.

|  |  |
| --- | --- |
| **KLIENTAS**  **Informatikos ir ryšių departamentas**  **prie Lietuvos Respublikos vidaus**  **reikalų ministerijos**  Direktorė  Viktorija Rūkštelė | **PASLAUGŲ TEIKĖJAS**  **UAB „Asseco Lietuva“**  Generalinis direktorius    Albertas Šermokas |