Pirkimo sąlygų 1 priedas „Techninė specifikacija"

ATSARGINIŲ KOPIJŲ PROGRAMINĖS ĮRANGOS COMMVAULT PALAIKYMO PASLAUGŲ TECHNINĖ SPECIFIKACIJA

1. VšĮ Lietuvos nacionalinis radijas ir televizija (toliau - Perkančioji organizacija/LRT) siekia įsigyti atsarginių kopijų programinės įrangos Commvault palaikymo paslaugas 12 mėn. laikotarpiui (toliau – Paslaugos). Reikalavimai Paslaugoms nurodyti šioje techninėje specifikacijoje.

REIKALAVIMAI PASLAUGAI:

2. LRT turimos ir naudojamos atsarginių kopijų programinės įrangos Commvault licencijos, kurioms perkamas palaikymas:

2.1. 25 vnt. VM Backup & Recovery Foundation - Per VM (10 Pack).

2.2. 15 vnt. Application Level Backup & Recovery - Per Client.

2.3. 20 vnt. File Level Backup & Restore with OnePass.

3. Paslaugos teikimo laikotarpis – 12 (dvylika) mėnesių nuo dabar LRT turimo ir galiojančio palaikymo pabaigos – 2026 m. rugsėjo 28 d. 00:00 val.

4. Paslauga turi būti teikiama ne mažiau kaip dviem lygiais:

4.1. I lygis – Tiekėjas, priimantis ir registruojantis pranešimus apie gedimus, atliekantis gedimų nustatymą, šalinimą bei su tuo susijusias paslaugas. O taip pat atsakingas už visą aptarnavimo proceso vykdymą ir valdymą.

4.2. II lygis – Įrangos gamintojas.

5. I lygio atstovas turi:

5.1. Užtikrinti gedimų ir problemų registravimą telefonu ir elektroniniu paštu[1].

5.2. Paslaugas turi teikti 24x7 (24 valandas per parą, 7 dienas per savaitę) principu.

5.3. Problemas privalo registruoti jas klasifikuojant ir paslaugą teikiant ne blogesniu kaip reakcijos laiku po pranešimo apie problemą:

5.3.1. reakcijos laikas ne ilgiau kaip 4 val., kai programinė įranga nustoja veikti.

5.3.2. reakcijos laikas ne ilgiau kaip 8 val., kai programinės įrangos sutrikimas gali įtakoti sistemos darbingumą;

5.3.3. reakcijos laikas ne vėliau kaip sekanti darbo diena, kai problema neturi įtakos sistemos darbingumui ir našumui.

5.4. Savo kompetencijos ribose privalo atlikti užregistruotų problemų indentifikavimą, jų šalinimą ir esant poreikiui perkėlimą į II paslaugos lygį.

5.5. Pagal poreikį turi diegti gamintojo teikiamus programinės įrangos atnaujinimus ar klaidų taisymus. Diegimas atliekamas pagal suderintą su Perkančiąja organizacija grafiką, atsižvelgiant į galimą sistemos stabdymo poreikį, galimus sutrikimus ir veikimo atstatymą nesėkmės atveju.

6. II lygio Paslaugos turi būti teikiamos programinės įrangos gamintojo.

7. II lygio atstovas turi teikti programinės įrangos palaikymą, klaidų šalinimą ir versijų atnaujinimą.

8. Paslauga gali būti teikiama lietuvių ir / arba anglų kalbomis. Pirmenybė teikiama lietuvių kalbai. Jeigu neįmanoma Paslaugos teikti lietuvių kalba, tuomet Paslauga teikiama anglų kalba.

KITI REIKALAVIMAI

9. Šis pirkimas laikomas žaliuoju pirkimu, kadangi pirkime taikomas Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo patvirtinto Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 (Lietuvos Respublikos aplinkos ministro 2022 m. gruodžio 13 d. įsakymo Nr. D1-401 redakcija) (toliau – aprašas), 4.4.3 papunktis - perkama nematerialaus pobūdžio paslauga, nesusijusi su materialaus objekto sukūrimu, kurios teikimo metu nėra numatomas reikšmingas neigiamas poveikis aplinkai, nesukuriamas taršos šaltinis ir negeneruojamos atliekos.

10. Šis pirkimas laikomas susijusiu su nacionaliniu saugumu, todėl šio pirkimo atžvilgiu keliami specialieji reikalavimai tiekėjo siūlomoms prekėms, nurodytoms šioje Techninėje specifikacijoje, siekiant užtikrinti šalies nacionalinio saugumo interesus. Nacionalinio saugumo reikalavimai paslaugoms nurodyti Specialiųjų Pirkimo sąlygų 4 skyriuje.

KIBERNETINIAI IR INFORMACIJOS SAUGUMO REIKALAVIMAI

11. Kibernetinio ir informacijos saugumo reikalavimai tiekėjui (toliau – KIS reikalavimai) yra neatskiriama techninės specifikacijos dalis. Jie apibrėžia minimalų kibernetinio ir informacijos saugumo lygį, kurį privalo užtikrinti Tiekėjas, vykdydamas su Perkančiąja organizacija sudarytą sutartį, kiek tai susiję su pirkimo objektu.

12. KIS reikalavimai yra parengti, atsižvelgiant į Lietuvos Respublikos kibernetinio saugumo įstatymą, Kibernetinio saugumo reikalavimų aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2024 m. lapkričio 6 d. nutarimu Nr. 945 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo" ir tarptautinius informacijos saugumo standartus ISO/IEC 27001:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai" ir ISO/IEC 27002:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės".

13. Tiekėjas, teikdamas pasiūlymą ir vykdydamas sutartį, patvirtina, kad yra susipažinęs su KIS reikalavimais, juos atitinka ir įsipareigoja jų laikytis visą sutarties galiojimo laikotarpį. Jeigu sutarties vykdymui bus pasitelkiami subteikėjai, Tiekėjas privalo užtikrinti, kad jie taip pat atitiktų jiems taikytinus KIS reikalavimus ir jų laikytųsi visą dalyvavimo vykdant sutartį laikotarpį.

14. Tiekėjas turi užtikrinti, kad jo darbuotojai, dalyvaujantys sutarties vykdyme: būtų supažindinti su Tiekėjo taikomais kibernetinio ir informacijos saugumo reikalavimais ir šioje techninėje specifikacijoje nustatytais KIS reikalavimais; būtų su Tiekėju pasirašę konfidencialumo pasižadėjimus ir (arba) susitarimus dėl informacijos neatskleidimo.

15. Tiekėjas sutinka gavęs Perkančiosios organizacijos prašymą, prieš sudarant sutartį arba sutarties vykdymo metu, neatlygintinai pateikti rašytinius įrodymus, patvirtinančius Tiekėjui taikomų KIS reikalavimų ar bet kurio iš taikomų reikalavimų įgyvendinimą.

16. Perkančioji organizacija sutarties vykdymo laikotarpiu turi teisę atlikti Tiekėjui taikomų KIS reikalavimų atitikties auditą (patikrinimą) arba pavesti jį atlikti trečiajai šaliai. Tiekėjas įsipareigoja neatlygintinai sudaryti sąlygas tokiam patikrinimui ir suteikti reikalingą informaciją bei prieigą tiek savo, tiek – jei taikoma – subtiekėjų veiklos apimtyje, kiek tai susiję su sutarties vykdymu.

17. Jeigu pasiūlymą pateikęs Tiekėjas yra Pasaulinis gamintojas[1], kurio informacijos saugumo atitikties įrodymai (ISO/IEC 27001, SOC 2 ar lygiaverčiai standartai) yra viešai skelbiami ir atitinka tarptautinius informacijos saugumo standartus, laikoma, kad KIS reikalavimų atitiktis yra pagrįsta šiais dokumentais, jeigu jie apima su pirkimo objektu susijusias paslaugas.

18. Jeigu Paslaugos yra Pasaulinio gamintojo, tačiau įsigyjamos per Tiekėją - tarpininką:

18.1. jei tarpininkas neturės prieigos prie tinklų ir (ar) Perkančiosios organizacijos informacinių sistemų ir neatliks jų konfigūravimo, administravimo ar diegimo veiksmų, KIS reikalavimai jam netaikomi;

18.2. jei tarpininkas turės prieigą prie tinklų ir (ar) Perkančiosios organizacijos informacinių sistemų arba atliks jų konfigūravimo, administravimo ar diegimo veiksmus, jam reikalavimai taikomi.

19. Tiekėjas įsipareigoja nedelsdamas, bet ne vėliau kaip per 2 darbo dienas, raštu informuoti Perkančiosios organizacijos už sutartį atsakingą asmenį, jei bet kuriuo metu nebeatitinka nustatytų KIS reikalavimų. LRT taip pat gali nustatyti neatitikimus savo iniciatyva arba remdamasi ir įvertinusi gautą informaciją iš trečiųjų šalių, įskaitant, bet neapsiribojant, kompetentingomis institucijomis. Nustačius neatitikimus, LRT suteikia protingą terminą jiems pašalinti, apie tai raštu informuodama Tiekėją. Tiekėjui per nustatytą terminą nepašalinus neatitikimų, Tiekėjas moka pirkimo sutartyje numatytus delspinigius iki kol neatitikimai bus pašalinti.

20. Jeigu sutarties vykdymui bus būtina suteikti Tiekėjui prieigą prie Perkančiosios organizacijos informacinių sistemų / išteklių, tokia prieiga bus suteikiama per Privilegijuotos prieigos valdymo sistemą (PAM), užtikrinančią prieigų stebėseną, audito įrašus, laikinumą ir centralizuotą kontrolę. PAM naudotojo paskyra suteikiama konkrečiam Tiekėjo darbuotojui tik tiek, kiek būtina sutarties vykdymui. Prieiga suteikiama tik laikotarpiui, reikalingam sutarties vykdymui, bet ne ilgesniam nei sutarties galiojimo laikotarpis. Tiekėjui draudžiama naudoti alternatyvius ar su Perkančiąja organizacija nesuderintus prisijungimo būdus.

[1] Pasaulinis gamintojas - tiekėjas, kuris: teikia informacines ar technologines paslaugas ar gamina įrangą, naudojamą tarptautiniu mastu (bent dviejuose žemynuose); yra plačiai žinomas tarptautiniu mastu kaip informacinių technologijų ar kibernetinio saugumo paslaugų teikėjas ar įrangos gamintojas; viešai skelbia galiojančius informacijos saugumo sertifikatus ar atitikties deklaracijas pagal tarptautinius standartus (ISO/IEC 27001, SOC 2, ENS arba lygiaverčius).

21. Jei atsiras papildomas poreikis suteikti prieigą, Tiekėjas privalės iš anksto, ne vėliau kaip prieš 5 darbo dienas, informuoti Perkančiąją organizaciją ir pagrįsti tokios prieigos būtinumą. Prieiga suteikiama tik Perkančiosios organizacijos sprendimu.

22. Tiekėjas turi užtikrinti, kad prieigos prie Perkančiosios organizacijos informacinių išteklių būtų suteikiamos tik tiems Tiekėjo darbuotojams (ar Tiekėjo pasitelktiems subtiekėjams), kurie susiję su sutarties vykdymu ir bus nedelsiant panaikintos, pasibaigus sutarčiai su Perkančiąja organizacija, pasibaigus Tiekėjo darbuotojo, kuriam buvo suteiktos prieigos prie Perkančiosios organizacijos informacinių išteklių, darbo santykiams su Tiekėju, pasibaigus subtiekėjo pasitelkimo pagrindui ar subtiekėjo sutartiniams santykiams su Tiekėju arba kai prieigos taps nereikalingos sutarties vykdymui.

23. Tiekėjui draudžiama perduoti ar dalintis jam suteiktomis prieigomis prie Perkančiosios organizacijos informacinių išteklių su trečiaisiais asmenimis, naudoti jas asmeniniais ar su sutarties vykdymu nesusijusiais tikslais, taip pat atlikti bet kokius veiksmus, pažeidžiančius kibernetinio saugumo ar kitų teisės aktų reikalavimus.

24. Jeigu sutarties vykdymo metu Tiekėjo darbuotojai (ar pasitelkti subtiekėjai), naudodami Tiekėjo valdomus įrenginius, jungsis prie Perkančiosios organizacijos informacinių sistemų ar išteklių arba tokiuose įrenginiuose tvarkys Perkančiosios organizacijos informaciją, Tiekėjas:

24.1. tokiuose įrenginiuose turi taikyti slaptažodžių politiką. Slaptažodžių politika turi nustatyti minimalų slaptažodžių sudėtingumo lygį – ne trumpesnį kaip 12 simbolių slaptažodį, sudarytą iš raidžių, skaičių ir specialiųjų simbolių, draudimą naudoti ankstesnius slaptažodžius ir jų periodinio keitimo tvarką – ne rečiau kaip kas 6 mėnesius. Politika turi numatyti, kad po nustatyto nesėkmingų prisijungimo bandymų skaičiaus, ne daugiau kaip 5 bandymų, prieiga būtų automatiškai užrakinama arba kitaip apribojama;

24.2. privalo užtikrinti, kad tokie įrenginiai būtų apsaugoti nuo neteisėtos prieigos, duomenų praradimo ir kenkėjiškos programinės įrangos. Tokiuose įrenginiuose turi būti taikomos šios saugumo priemonės: įrenginiuose saugomų duomenų šifravimas, automatinis ekrano užrakinimas, apsauga nuo kenkėjiškos programinės įrangos, operacinių sistemų ir programinės įrangos saugumo atnaujinimų diegimas.

25. Jeigu sutarties vykdymo metu Tiekėjo darbuotojai ar pasitelkti subtiekėjai, naudodami Tiekėjo valdomą įrangą, operacines sistemas ar programinę įrangą, jungsis prie Perkančiosios organizacijos informacinių sistemų ar išteklių arba tvarkys Perkančiosios organizacijos informaciją, tokia įranga, operacinės sistemos ir programinė įranga turi būti naudojamos teisėtai, jų gyvavimo ciklas neturi būti pasibaigęs ir joms turi būti teikiamas gamintojo palaikymas.

26. Ne vėliau kaip per 5 darbo dienas nuo sutarties pabaigos, Tiekėjas turi (išskyrus, jei duomenys negali būti sunaikinti ar ištrinti dėl teisinių, reguliacinių ar kitų pagrįstų priežasčių (pvz., teisės aktų nustatyto saugojimo termino, teisėto duomenų tvarkymo pagrindo ar vykdomo tyrimo)):

26.1. sunaikinti visus Perkančiosios organizacijos perduotus, sutarties vykdymo metu gautus duomenis, išskyrus atvejus, kai Perkančioji organizacija reikalauja juos grąžinti arba perkelti nurodytam trečiajam asmeniui – kitam duomenų tvarkytojui;

26.2. ištrinti asmens duomenis pagal Bendrojo duomenų apsaugos reglamento (BDAR) ir kitų teisės aktų reikalavimus;

26.3. grąžinti visas Perkančiosios organizacijos suteiktas laikinas prieigos, technines ar informacines priemones (jeigu tokių buvo suteikta).

27. Tiekėjas turi turėti dokumentuotas kibernetinių ir informacijos saugumo incidentų valdymo procedūras, apimančias incidentų identifikavimą, reagavimą, dokumentavimą ir informavimą. Kibernetiniu ar informacijos saugumo incidentu laikomas bet koks įvykis ar tarpusavyje susijusių įvykių seka, kuris (-ie) sutarties vykdymo metu sukelia arba gali sukelti neigiamą poveikį Perkančiosios organizacijos informacinėms sistemoms arba Perkančiosios organizacijos duomenų konfidencialumui, vientisumui ar prieinamumui. Apie šiame punkte nurodytus incidentus Tiekėjas privalo nedelsdamas, kai tik apie juos sužino, neatlygintinai informuoti Perkančiosios organizacijos kibernetinio saugumo vadovą el. paštu ciso@lrt.lt ir telefonu +370 602 48636.

28. Tiekėjas privalo neatlygintinai teikti informaciją apie incidento eigą iki jo galutinio išsprendimo, laikantis su Perkančiąja organizacija sutarto informacijos teikimo termino. Šis terminas nustatomas tuo metu, kai Tiekėjas informuoja apie įvykusį incidentą.

29. Apie incidento suvaldymą Tiekėjas privalo nedelsdamas, kai tik incidentas suvaldytas, informuoti Perkančiosios organizacijos kibernetinio saugumo vadovą el. paštu ciso@lrt.lt ir telefonu +37060248636.

30. Incidento atveju, jei nustatoma, kad pažeidimas kilo dėl Tiekėjo kaltės (veikimo ar neveikimo), vykdant Sutartį, Tiekėjas atsako už Perkančiajai organizacijai padarytą tiesioginę žalą, kuri yra tiesioginė Tiekėjo veiksmų ar neveikimo pasekmė Sutartyje nustatyta tvarka ir apimtimi.