

NUTANIX CLUSTER SERVERIŲ TECHNINIO PALAIKYMŲ IR PROGRAMINĖS ĮRANGOS LICENCIJŲ PRATĖSIMO PIRKIMO TECHNINĖ SPECIFIKACIJA

1. VšĮ Lietuvos nacionalinis radijas ir televizija (toliau – Perkančioji organizacija; LRT) siekia įsigyti 12 mėnesių Nutanix virtualizacijos licencijų pratęsimą ir gamintojo techninės įrangos garantijos pratęsimą turimiems Nutanix HCI serveriams
2. Informacija apie įrangą, kuriai turi būti pratęstas gamintojo techninis palaikymas pateikiamas 1 lentelėje):

1 lentelė. Informacija apie įrangą

Eil. Nr.	Įrangos modelis	Serijinis numeris	Įsigijimo data:	Techninio palaikymo pabaigos data
2.1.	XF8055 M3	EWAA018649	2023-12-14	2026-12-13
2.2.	XF8055 M3	EWAA018650	2023-12-14	2026-12-13
2.3.	XF8055 M3	EWAA018651	2023-12-14	2026-12-13

3. Informacija apie Nutanix programinę įrangą, kuriai turi būti pratęstas gamintojo techninis palaikymas pateikiamas 2 lentelėje):

2 lentelė. Informacija apie Nutanix programinę įrangą

Eil. Nr.	Licencijos pavadinimas	Licencijos ID	Licencijos metrika	Įsigijimo data	Galiojimo pabaigos data
3.1.	NCI Starter, NCM Starter	LIC-02574648, LIC-02563009	72 CPU cores	2023-12-14	2026-12-13

4. Perkamas gamintojo įrangos techninio palaikymo ir licencijų pratęsimo terminas: nuo 1 ir 2 lentelėse nurodyto palaikymo pabaigos. Gamintojo suteikiamas techninio palaikymo ir atnaujintų licencijų galiojimo terminas ne trumpesnis kaip 12 mėn.
5. Pratęsiant 1 lentelėje išvardintos įrangos techninį palaikymą turi būti išlaikytos visos šiuo metu įrangoje registruotos licencijos. Jei pas gamintoją yra registruotų licencijų, kurių galiojimas baigiasi 1 lentelėje nurodytu terminu, bet techninėje specifikacijoje nepaminėtas, Tiekėjas privalo į pasiūlymo kainą įskaičiuoti tokių licencijų galiojimo pratęsimą ne trumpesniame kaip 12 mėn. laikotarpiui. Po gamintojo techninio palaikymo pratęsimo, techninio palaikymo sąlygos turi išlikti tokios pačios ar būti geresnės nei dabar galiojančios (jos negali būti pablogintos).
6. Techninio palaikymo galiojimo metu turi būti užtikrintas sugedusios techninės ir programinės įrangos remontas arba techninės arba programinės įrangos pakeitimas lygiaverčiu, programinės įrangos naujų versijų, pataisymų pateikimas, techninės pagalbos ir konsultacijų teikimas.
7. Tiekėjas, sutarties laikotarpiu, gedimo atveju privalo užtikrinti 1 ir 2 lentelėse išvardintos įrangos aukšto patikimumo telkinio (angl. Cluster) remontą ir konfigūracijos atstatymą.
8. Visų techninių fizinės įrangos komponentų gedimo atveju, gamintojas turi nemokamai juos pakeisti, o Tiekėjas atsako už proceso organizavimą. Sugedusių dalių siuntimas ir keitimas neturi būti papildomai apmokestinamas. Sugedusių dalių keitimas turi būti atliekamas Perkančiosios organizacijos patalpose, įrangos veikimo vietoje, nesutrikdant ar kitaip nepaveikiant įrangos veikimo.
9. Techninio palaikymo galiojimo metu turi būti užtikrintas prieiga prie įrangos techninės dokumentacijos, mokymosi resursų.
10. Dėl techninės pagalbos suteikimo, į gamintoją arba Tiekėją, turi būti galima kreiptis registruojant užklausą internetu arba telefonu. Problemų ir paklausimų registracija turi būti galima visą parą.

Kiti reikalavimai:

5. Perkančioji organizacija šiuo pirkimu siekia įsigyti Paslaugas, kurios daro mažesnę poveikį aplinkai viename ar keliuose paslaugų teikimo etapuose, todėl vadovaujantis LR aplinkos ministro 2011 m. birželio 28 d. įsakymo Nr. D1-508 „Dėl Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo patvirtinimo“ patvirtinto Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo 4.4.3 punktu, šiuo pirkimu yra įsigyjama tik nematerialaus pobūdžio (intelektinė) ar kitokia Paslauga, nesusijusi su materialaus objekto sukūrimu, kurios teikimo metu nėra numatomas reikšmingas neigiamas poveikis aplinkai, nesukuriamas taršos šaltinis ir negeneruojamos atliekos. Paslaugos teikiamos elektroniniu būdu.

Nacionalinio saugumo reikalavimai

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

Kvalifikacija

7. Pirkimo sutarties vykdymui, tiekėjas (tiekėjų grupės partneriai kartu), turi pasiūlyti bent vieną specialistą, tenkinantį šiuos nurodytus reikalavimus:

- 7.1. Specialistas turi turėti tiekėjo pasiūlytos programinės įrangos gamintojo „Master“ ar aukštesnio lygio specialisto kvalifikaciją.

Kvalifikacijos atitikimo įvertinimui tiekėjas turi pateikti tiekėjo specialistui gamintojo išduotą Master lygio sertifikatą.

Kibernetinio ir informacijos saugumo reikalavimai

8. Kibernetinio ir informacijos saugumo reikalavimai Tiekėjui (toliau – KIS reikalavimai) apibrėžia minimalų kibernetinio ir informacijos saugumo lygį, kurį privalo užtikrinti Tiekėjas, vykdydamas su Perkančiąja organizacija sudarytą sutartį, kiek tai susiję su pirkimo objektu.
9. 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“.
10. 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.
11. Tiekėjas sutinka gavęs Perkančiosios organizacijos prašymą, prieš sudarant sutartį arba sutarties vykdymo metu, neatlygintinai pateikti rašytinius įrodymus, patvirtinančius KIS reikalavimų įgyvendinimą.
12. Tiekėjas privalo iš anksto, ne vėliau kaip prieš 10 (dešimt) darbo dienų iki planuojamo pokyčio, raštu pranešti už sutartį atsakingam Perkančiosios organizacijos darbuotojui apie visus esminius Paslaugos teikimo pokyčius, kurie gali turėti įtakos Perkančiosios organizacijos informacijos, informacinių sistemų ar paslaugų konfidencialumui, vientisumui, prieinamumui, atsekamumui, sutartinių reikalavimų laikymuisi ar paslaugų tęstinumui. Perkančioji organizacija, gavusi informaciją, turi įvertinti pokyčio poveikį saugumui, bei gali iš Tiekėjo reikalauti papildomų saugumo priemonių arba, kraštutiniu atveju, nesutikti su pokyčiu.
13. 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.
14. 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 – subtiekjų veiklos apimtyje, kiek tai susiję su vykdoma sutartimi.

15. 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.
16. Tiekėjo naudojama įranga, operacinės sistemos ir programinė įranga, naudojama sutarties vykdymui, turi būti teisėta, nepasibaigusio gyvavimo ciklo ir turėti gamintojo palaikymą.
17. Tiekėjas privalo nedelsdamas, bet ne vėliau kaip per 3 darbo dienas nuo sužinojimo, informuoti Perkančiąją organizaciją apie su Paslauga susijusius pažeidžiamumus, galinčius turėti poveikį Perkančiosios organizacijos tinklų ar informacinių sistemų saugumui, bei pateikti informaciją apie jų šalinimo ar rizikos mažinimo priemones.
18. Jeigu Perkančioji organizacija nustato arba iš kitų šaltinių gauna informaciją apie pažeidžiamumą, susijusį su Paslauga, ir apie jį informuoja Tiekėją, Tiekėjas ne vėliau kaip per 3 darbo dienas privalo pateikti pažeidžiamumo įvertinimą ir informaciją apie gamintojo rekomenduojamas pažeidžiamumo šalinimo ar rizikos mažinimo priemones.
19. Apie nustatytus kritinius pažeidžiamumus, susijusius su Paslauga, Tiekėjas privalo informuoti Perkančiąją organizaciją nedelsdamas, bet ne vėliau kaip per 2 darbo dienas nuo sužinojimo apie juos, ir pateikti informaciją apie gamintojo rekomenduojamas pažeidžiamumo šalinimo ar rizikos mažinimo priemones.
20. Kritiniu pažeidžiamumu laikomas pažeidžiamumas, kuriam pagal galiojančią CVSS metodikos versiją suteiktas ne mažesnis kaip 9,0 balų įvertinimas, kuris įtrauktas į viešai skelbiamus aktyviai išnaudojamų pažeidžiamumų sąrašus arba kuris, atsižvelgiant į gamintojo, programinės įrangos tiekėjo, kompetentingos institucijos paskelbtą informaciją ar Perkančiosios organizacijos atliktą rizikos vertinimą, gali turėti reikšmingą poveikį Perkančiosios organizacijos tinklų ir informacinių sistemų saugumui.
21. Jeigu dėl objektyvių techninių ar organizacinių priežasčių šiame skyriuje nustatytais terminais informacijos pateikti nėra galimybės, terminas gali būti pratęstas šalių rašytiniu susitarimu.
22. Jei sutartinių įsipareigojimų vykdymui bus būtina jungtis prie Perkančiosios organizacijos informacinių išteklių, Perkančioji organizacija Tiekėjui prieigą suteiks per Privilegiuotos prieigos valdymo sistemą (PAM), užtikrinančią prieigų stebėseną, audito įrašus, laikinumą ir centralizuotą kontrolę. PAM naudotojo paskyra bus suteikiama konkrečiam Tiekėjo darbuotojui sutarties vykdymui. Prieiga suteikiama tik tokiam laikotarpiui, kuris reikalingas sutarties vykdymui, bet ne ilgesniam terminui nei sutarties galiojimo pabaiga. Tiekėjui draudžiama naudoti alternatyvius ar nesuderintus prisijungimo būdus.
23. 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.
24. Tiekėjas turi užtikrinti, kad prieigos prie Perkančiosios organizacijos informacinių išteklių būtų suteikiamos tik tiems Tiekėjo darbuotojams (ar Tiekėjo pasitelktiems subtiekjams), 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 subtiekjų pasitelkimo pagrindui ar subtiekjų sutartiniams santykiams su Tiekėju arba kai prieigos taps nereikalingos sutarties vykdymui.
25. 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.
26. Tiekėjas privalo užtikrinti, kad įrenginiai, iš kurių jungiamasi prie Perkančiosios organizacijos informacinių išteklių arba kuriuose tvarkoma su sutarties vykdymu susijusi Perkančiosios organizacijos informacija, būtų apsaugoti nuo neautorizuotos prieigos, duomenų praradimo ir kenkėjiškos programinės įrangos. Tokiuose įrenginiuose turi būti taikomas duomenų šifravimas, automatinis ekrano užrakinimas, apsauga nuo kenkėjiškos programinės įrangos ir diejami operacinių sistemų bei programinės įrangos saugumo atnaujinimai.
27. Tiekėjas turi turėti dokumentuotas veiklos tęstinumo procedūras, leidžiančias užtikrinti sutartinių įsipareigojimų vykdymą jo veiklos sutrikimų, incidentų ar kitų nenumatytų aplinkybių atveju, kiek tai susiję su sutarties vykdymu.

28. 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 informaciniams ištekliams, jos duomenų konfidencialumui, vientisumui ar prieinamumui. Apie incidentus, nurodytus šiame punkte, Tiekėjas privalo nedelsdamas ir neatlygintinai, kai tik sužino apie tokį incidentą, informuoti Perkančiosios organizacijos kibernetinio saugumo vadovą el. paštu: ciso@lrt.lt ir telefonu +37060248636.
29. 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.
30. Apie incidento suvaldymą Tiekėjas privalo nedelsdamas, kai tik incidentas suvaldytas, informuoti Perkančiosios organizacijos kibernetinio saugumo vadovą el. paštu ciso@lrt.lt ir telefonu +37060248636.
31. Tiekėjas galutinę incidento tyrimo ataskaitą ar ataskaitos dalį (jeigu ataskaita yra susijusi ne tik su Perkančiąja organizacija) turi neatlygintinai pateikti ne vėliau kaip per 3 darbo dienas nuo incidento suvaldymo el. paštu ciso@lrt.lt.
32. Tiekėjas turi bendradarbiauti su Perkančiąja organizacija ir priežiūros institucijomis bei neatlygintinai teikti visą būtiną informaciją tyrimams, susijusiems su kibernetiniu, informacijos saugumu, asmens duomenų apsauga ar incidentais, kiek tai susiję su sutarties ar pažeidimo vykdymu (tyrimu). Paslaugų teikėjas privalo pateikti reikalaujamą informaciją per Perkančiosios organizacijos numatytą terminą.
33. Tiekėjas prisiima atsakomybę už savo, savo darbuotojų, subteikėjų (jei jie būtų su pasitelkti) veiksmus ir neveikimą, susijusius su šių KIS reikalavimų įgyvendinimu, kiek jie yra susiję su sutarties vykdymu ir sutartyje nustatyta atsakomybe.