[redacted]

DUOMENŲ ATSARGINIŲ KOPIJŲ SISTEMOS, DIEGIMO IR MOKYMO PASLAUGŲ TECHNINĖ SPECIFIKACIJA

Pirkimo objektas – *Duomenų atsarginių kopijų sistema (toliau – sistema), diegimo ir mokymo paslaugos*. Nacionalinio kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – perkančioji organizacija) numato įsigyti du įrenginius, kurie sudarytų bendrą atsarginių kopijų sistemą. Sistema skirta perkančiosios organizacijos Vilniaus ir Kauno duomenų centrų (KSIS paslaugų) elektroninės informacijos ir jos atsarginių kopijų apsaugai. Kibernetinio saugumo informacinė sistema (KSIS) yra skirta kaupti ir apdoroti kibernetinių incidentų aptikimo duomenis, dalytis informacija apie galimus ir įvykusius kibernetinius incidentus bei kita kibernetinio pobūdžio informacija.

Santrumpų išaiškinimas

- **Mazgas –** įrenginys (komponentas) apimantis procesorių, atmintį, diskinį ir tinklinį resursus (angl. *node*);
- **Telkinys –** mazgai, apjungiantys savo resursus į bendrą visumą sudaro aukšto našumo ir patikimumo telkinį (bendra skaičiavimo galia, bendra diskinė talpa, bendros funkcijos, unifikuotas valdymas) (angl. *cluster*);
- **Sistema –** telkinių visuma, išdėstyta skirtinguose duomenų centruose ir naudojanti duomenų perkėlimo technologijas informacijos apsaugai užtikrinti nuo gaisro, vandens ir kitų rizikos veiksnių (angl. *system*);
- **KMIP –** kriptografinių raktų valdymo protokolas (angl. *Key Management Interoperability Protocol*);
- **HDD –** magnetinis diskas (angl. *Hard Disk Drive*);
- **SSD –** puslaidininkinis diskas (angl. *Solid State Drive*);
- **CMVP –** jungtinė JAV ir Kanados kriptografinių modulių saugumo patikrinimo programa (angl. *Cryptographic Module Validation Program*);
- **TLS –** transporto lygmens saugos protokolas (angl. *Transport Layer Security*);
- **SFP** arba **SFP+ -** tinklo prievado modulis (angl. S*mall Form-factor Pluggable*);
- **NTP –** tinklinis laiko protokolas (angl. *Network Time Protocol*);
- **HTML –** hiperteksto ženklinimo kalba (angl. *HyperText Markup Language*);
- **SSH –** saugios konsolės administravimo protokolas (angl. *Secure Shell Protocol*);
- **LDAP –** informacinių direktorijų prieigos protokolas (angl. *Lightweight Directory Access Protocol*);
- **PDU –** elektros šakotuvas (angl. *Power Distribution Unit*);
- **NFS –** tinklinė failų sistema (angl. *Network File System*);

	Pirkimo dokumentuose nurodyta reikšmė	Pildo tiekėjas
1.	**Bendrieji reikalavimai:**	**-**
1.1	Tiekėjas turi būti siūlomos įrangos gamintojas arba gamintojo atstovas arba sudaręs sutartį su tokiu atstovu. Tiekėjas, atstovaujantis gamintoją tiesiogiai arba veikiantis per gamintojo atstovą, kartu su pasiūlymu turi pateikti gamintojo ar jo atstovo pažymą, kad yra įgaliotas pateikti (parduoti) siūlomą įrangą. Pažymoje gamintojas ar jo atstovas taipogi turi patvirtinti, kad siūloma prekė yra sukomplektuota perkančiajai organizacijai. Jei pasiūlymą teikia pats gamintojas, pakanka patvirtinimo, kad siūloma prekė yra sukomplektuota perkančiajai organizacijai. Dokumentai gali būti teikiami lietuvių arba anglų kalbomis;	*Žr. dokumentą: Blue Bridge MSP - letter_of_authorization.pdf ir Rubrik patvirtinimas_EN.pdf*
1.2.	visa pateikiama techninė įranga privalo būti nauja (negali būti atnaujinta, restauruota (angl. *refurbished*)), turi būti nenaudota, pateikta nepažeistoje gamyklinėje pakuotėje;	
1.3.	Tiekėjas turi užtikrinti, kad nėra paskelbta žinia apie siūlomos įrangos gamybos arba tobulinimo nutraukimą (pvz., angl. *End of Lifetime* ar *Discontinued*);	
1.4.	kartu su pasiūlymu Tiekėjas turi pateikti nuorodą į gamintojo viešai prieinamą svetainę, kurioje yra tikslios pasiūlymą atitinkančio produkto techninės charakteristikos arba turi būti pridėtas parengtas dokumentas su siūlomo produkto techninėmis charakteristikomis;	*Pateikiami gamintojo dokumentai:* *Rubrik R7000 appliance specifications.pdf* *Rubrik R7000 Hardware Guide (A1).pdf* *Rubrik licensing guide.pdf* *Rubrik Compatibility Matrix (May 29, 2025).pdf* *Rubrik support policy.pdf* *Rubrik premium support.pdf* *Rubrik CDM Version 9.3 Install Guide (Rev. A0).pdf* *Rubrik CDM Version 9.3 User Guide (Rev. A3).pdf* *Rubrik CDM Version 9.3 Security Guide (Rev. A0).pdf* *Rubrik CDM Version 9.3 Events Guide (Rev. A0).pdf* *Rubrik CDM Version 9.3 CLI Guide (Rev. A0).pdf* *Rubrik CDM Version 9.3 Cloud Cluster Setup Guide (Rev. A3).pdf* *Rubrik Security Cloud User Guide - June 23, 2025.pdf* *Rubrik Security Cloud Offline Recovery Guide - CDM Version 9.3 (Rev. A0).pdf* *Rubrik anomaly detection data sheet.pdf* *Rubrik and VMware vSphere - reference architecture.pdf*

1.5.	įrangos dokumentai turi būti lietuvių arba anglų kalba. Užrašai ant įrenginio ir jo dalių turi būti lietuvių arba anglų kalba. Gamintojo interneto svetainėje tvarkyklių ir dokumentų paieška atliekama lietuvių arba anglų kalba;	*Anglų kalba.*
1.6.	Tiekėjas į savo pasiūlymą turi įtraukti visą techninę ir programinę įrangą bei eksploatacines medžiagas, reikalingas šioje specifikacijoje nurodytiems reikalavimams įvykdyti;	
1.7.	visos būtinos licencijos turi būti įskaičiuotos į pasiūlymo kainą. Licencijų galiojimas turi būti ne trumpesnis nei įrangai reikalaujamas garantinio aptarnavimo laikotarpis (2.19 p.);	*Visos licencijos įskaičiuotos į kainą, licencija: RS-BT-EE-PE-PP - Rubrik Enterprise Edition, Premium support, per usable BETB – 120TB, 60 mėnesių;*
1.8.	saugumo reikalavimai: • magnetiniai ar puslaidininkiniai diskai (angl. *HDD/SSD*) ar kitos atminties laikmenos gedimo atveju turi būti keičiamos naujomis. Sugedusios atminties laikmenos sunaikinamos perkančiosios organizacijos patalpose ir Tiekėjui negrąžinamos; • įrangos gedimo atveju iš nuolatinės eksploatacijos vietos remontui išvežamą sugedusią įrangą perkančioji organizacija pateikia be joje sumontuotų magnetinių ar puslaidininkinių diskų (angl. *HDD/SSD*) ar kitų atminties laikmenų; • Tiekėjas turi užtikrinti, kad įsigyjamoje įrangoje nebūtų įdiegta jokios papildomos programinės įrangos, kuri nėra būtina tokios įrangos funkcionalumui užtikrinti. Paaiškėjus, kad įrangoje yra įdiegta įtartina, šnipinėjimo ar kokia kita kenkimo programinė įranga, tai būtų traktuojama kaip Sutarties reikalavimų nesilaikymas. Tokiu atveju įranga grąžinama Tiekėjui arba keičiama nauja lygiaverte ar geresnių parametrų, tačiau saugumo reikalavimus atitinkančia įranga;	
1.9.	pirkimo objektas, vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo 37 str. 8 d. ir 9 d. bei 10 d. numatyta išimtimi, turi nekelti grėsmės nacionaliniam saugumui;	
2.	**Reikalavimai duomenų atsarginių kopijų sistemai**	**-**
2.1.	**Gamintojas:** nurodyti gamintoją;	*Rubrik.*
2.2.	**Produkto pavadinimas:** nurodyti produkto pavadinimą, modelį;	*Rubrik R7000 appliance, R7408.*
2.3.	**Fizinės savybės:** fizinė įranga turi tilpti į perkančiosios organizacijos turimą 450 mm pločio ir 914,40 mm gylio spintą. Turi būti pateikti visi reikiami montavimo į spintą komponentai (bėgeliai, tvirtinimo varžtai ir t.t.). Jei gamintojas yra numatęs kabelių prilaikančiąją dalį (angl. *cabling management arm*), ji turi būti pasiūlyta;	*Fizinės savybės:* *fizinė įranga telpa į perkančiosios organizacijos turimą 450 mm pločio ir 914,40 mm gylio spintą (aukštis - 88 mm, plotis - 449 mm, gylis - 775 mm). Pateikti visi reikiami montavimo į spintą komponentai (bėgeliai, tvirtinimo varžtai ir t.t.). Gamintojas nenumato kabelių prilaikančiosios dalies (angl. cabling management arm).*
2.4.	**Sistema:**	

	siūloma sistema turi būti sudaryta iš dviejų telkinių. Visi siūlomi komponentai privalo būti pateikti vieno gamintojo arba skirtingų gamintojų suderinti bendram darbui;	
2.5.	**Telkiniai:** turi būti sudaryti iš mazgų. Telkiniai turi toleruoti bet kokio mazgo ar jo komponento gedimą. Turi būti galimybė telkinius išplėsti papildomais mazgais nestabdant telkinių darbo. Kiekvieno siūlomo telkinio operatyviosios atminties kiekis turi būti ne mažesnis nei 512 GB ir atminties technologija ne prastesnė nei DDR5 arba lygiavertė;	*Telkinys Nr. 1* *R7408 telkinys yra sudarytas iš 4 mazgų, toleruoja bet kokio mazgo ar jo komponento gedimą, yra galimybė išplėsti telkinį papildomais mazgais nestabdant telkinio darbo.* *Siūlomo telkinio charakteristikos:* *Procesorius: 4 x Intel 12-Core x86 30 MB Cache, 2.0 GHz* *Atmintis: 768 GB DDR5* *Diskai: 12 x 8 TB HDD ir 8 x 3.84 TB SSD* *Tinklo jungtys: 4x Quad-Port 10 GbE/25 GbE, komplektuojamos 25GBase-SR SFP28 spinduliuokliais ir 4x 1 GbE (IPMI)* *Naudinga talpa: 60 TB* *Telkinys Nr. 2* *R7408 telkinys yra sudarytas iš 4 mazgų, toleruoja bet kokio mazgo ar jo komponento gedimą, yra galimybė išplėsti telkinį papildomais mazgais nestabdant telkinio darbo.* *Siūlomo telkinio charakteristikos:* *Procesorius: 4x Intel 12-Core x86 30 MB Cache, 2.0 GHz* *Atmintis: 768 GB DDR5* *Diskai: 12x 8 TB HDD ir 8x 3.84 TB SSD* *Tinklo jungtys: 4x Quad-Port 10 GbE/25 GbE, komplektuojamos 25GBase-SR SFP28 spinduliuokliais ir 4x 1 GbE (IPMI)* *Naudinga talpa: 60 TB* *Rubrik užtikrina klasterio (cluster) atsparumą gedimams, apsaugant nuo diskų ir komponentų gedimų keliais pagrindiniais mechanizmais:* *• Erasure Coding: „Rubrik“ naudoja 4:2 erasure coding, paskirstydama duomenis tarp kelių diskų ir mazgų (nodes). Net sugedus dviems diskams, duomenys išlieka prieinami ir atkuriami.* *• Self-Healing Mechanisms: Diskui sugedus, „Rubrik“ automatiškai atkuria duomenų rinkinius kituose prieinamuose diskuose, taip užtikrindama nepertraukiamą paslaugų prieinamumą.*

		• Immutable File System (Atlas): failų sistema užkerta kelią duomenų sugadinimui, nes kartą įrašyti duomenys nebegali būti modifikuojami ar ištrinami. *• Cluster-Based Architecture: „Rubrik“ telkiniai sudaryti bent iš keturių mazgų (nodes), kurių kiekvienas turi savo saugyklos (storage), tinklo (network) ir skaičiavimo (compute) resursus. Duomenys paskirstomi tarp šių mazgų, taip užtikrinant jų dubliavimą (redundancy).* *• Live Disk Replacement: Sugedę diskai gali būti pakeisti tuo metu, kai mazgas (node) veikia, išlaikant bendrą saugyklos pajėgumą be prastovų (downtime).*
2.6.	**Mazgai:** siūlomas procesorius mazguose turi būti x86-64 ar lygiavertės architektūros. Nurodyti siūlomų mazgų charakteristikos parametrus ir kiekius kiekviename telkinyje;	*Telkinys Nr. 1* *Siūlomų mazgų kiekis - 4* *Siūlomų mazgų charakteristikos parametrai (kiekvieno mazgo):* *Procesorius: 1x Intel 12-Core x86 30 MB Cache, 2.0 GHz* *Atmintis: 192 GB DDR5* *Diskai: 3x 8 TB HDD ir 2x 3.84 TB SSD* *Tinklo jungtys: 1x Quad-Port 10 GbE/25 GbE, komplektuojamos 25GBase-SR SFP28 spinduliuokliais ir 1x 1 GbE (IPMI)* *Telkinys Nr. 2* *Siūlomų mazgų kiekis - 4* *Siūlomų mazgų charakteristikos parametrai (kiekvieno mazgo):* *Procesorius: 1x Intel 12-Core x86 30 MB Cache, 2.0 GHz* *Atmintis: 192 GB DDR5* *Diskai: 3x 8 TB HDD ir 2x 3.84 TB SSD* *Tinklo jungtys: 1x Quad-Port 10 GbE/25 GbE, komplektuojamos 25GBase-SR SFP28 spinduliuokliais ir 1x 1 GbE (IPMI)*
2.7.	**Naudinga talpa:** kiekvieno sistemą sudarančio telkinio naudinga talpa po diskų agregavimo turi būti ne mažesnė nei 60 TB dydžio. Licencijos turi būti pateiktos visai siūlomai naudingai talpai, jei tokios yra būtinos. Turi būti galimybė kiekvieno telkinio naudingą talpą išplėsti iki ne mažiau nei 360 TB dydžio nestabdant telkinių	*Telkinys Nr. 1* *Naudinga talpa – 60 TB* *Naudingos talpos plėtimo galimybės – R7408 modelio bazinį telkinį sudaro 1 BRIK, kuriame yra 4 mazgai, jo naudinga talpa yra 60TB. Gamintojas nenustato ribojimo maksimaliam mazgų kiekiui, telkinys gali*

	darbo (bendra sistemos naudinga talpa turi būti plečiama iki ne mažiau nei 720 TB). Duomenys turi būti apsaugoti nuo bet kurių dviejų diskų gedimo vienu metu. Nurodyti siūlomą naudingą talpos dydį kiekvienam telkiniui atskirai, naudingos talpos plėtimo galimybes, juos sudarančių diskų dydį, kiekį ir siūlomą duomenų apsaugos mechanizmą kiekvienam telkiniui atskirai, atitinkantį keliamas sąlygas;	*būti plečiamas "scale out" būdu, prijungiant papildomų mazgų pagal poreikį, todėl telkinio naudingą talpą galima plėsti iki 360 TB ir daugiau.* *Licencija yra pagal telkinio talpą, kiekis – 60 TB* *Diskų dydis ir kiekis - 12x 8 TB HDD ir 8x 3.84 TB SSD* *Duomenų apsaugos mechanizmas – erasure coding, duomenys apsaugoti nuo bet kurių dviejų diskų gedimo vienu metu* *Telkinys Nr. 2* *Naudinga talpa – 60 TB* *Naudingos talpos plėtimo galimybės – R7408 modelio bazinį telkinį sudaro 1 BRIK, kuriame yra 4 mazgai, jo naudinga talpa yra 60TB. Gamintojas nenustato ribojimo maksimaliam mazgų kiekiui, telkinys gali būti plečiamas "scale out" būdu, prijungiant papildomų mazgų pagal poreikį, todėl telkinio naudingą talpą galima plėsti iki 360 TB ir daugiau.* *Licencija yra pagal telkinio talpą, kiekis – 60 TB* *Diskų dydis ir kiekis - 12x 8 TB HDD ir 8x 3.84 TB SSD* *Duomenų apsaugos mechanizmas – erasure coding, duomenys apsaugoti nuo bet kurių dviejų diskų gedimo vienu metu*
2.8.	**Duomenų glaudinimas:** telkiniai privalo palaikyti dublikatų naikinimo ir duomenų suspaudimo funkcijas (angl. *deduplication and compression*). Jei šios funkcijos yra licencijuojamos, turi būti pateiktos visos reikalingos licencijos, atrakinančios šį funkcionalumą be jokių apribojimų. Abi funkcijos privalo veikti vienu metu. Duomenų dublikatų naikinimas turi būti atliekamas automatiškai, be administratoriaus įsikišimo. Duomenų suspaudimas gali būti kaip papildomai pasirenkama funkcija;	*Telkinys Nr. 1* *Siūlomas telkinys palaiko dublikatų naikinimo ir duomenų suspaudimo funkcijas (angl. deduplication and compression), funkcionalumas įeina į bazinę licenciją.* *Telkinys Nr. 2* *Siūlomas telkinys palaiko dublikatų naikinimo ir duomenų suspaudimo funkcijas (angl. deduplication and compression), funkcionalumas įeina į bazinę licenciją.* *Rubrik naudoja suspaudimo (compression) ir deduplikavimo (deduplication) technologijas, taip optimizuojant duomenų saugyklos efektyvumą ir sumažinant duomenims saugoti reikalingą talpą. Veikimo principai:*

		• Global Deduplication: Rubrik pašalina duomenų pasikartojimą visame klasteryje (cluster), užtikrinama, kad būtų saugomi tik unikalūs duomenų blokai (blocks). *• Incremental Forever: Rubrik išsaugo tik tuos duomenis, kurie pakito nuo paskutinės atsarginės kopijos (backup) darymo, taip sumažinamas saugojimo vietos poreikis ir padidindamas efektyvumas.* *• Cascading Cross Deduplication: ši funkcija pagerina deduplikavimą, leisdama keliems klasteriams (clusters) tarpusavyje deduplikuoti persidengiančias pilnas atsargines kopijas (full backups).* *• Compression Optimization: Rubrik taiko išmanųjį suspaudimą (intelligent compression), mažindamas duomenų užimamą vietą, kartu išlaikant duomenų vientisumą (data integrity).* *Šios technologijos veikia automatiškai ir užtikrina efektyvų duomenų saugyklų naudojimą, mažina išlaidas ir pagerina atsarginių kopijų (backup) našumą.*
2.9.	**Sauga:**	
2.9.1.	telkiniai saugomų duomenų šifravimui turi palaikyti AES-256 ar lygiavertį kriptografinį algoritmą. Įrenginio kriptografinė biblioteka turi būti sertifikuota pagal CMVP (angl. *Cryptographic Module Validation Program)* ar lygiavertę patikrinimo programą. Kriptografinei bibliotekai turi būti išduotas galiojantis sertifikatas pasiūlymo pateikimo dieną. Pateikti sertifikato numerį ir/arba nuorodą į sertifikatą, kuris paskelbtas CMVP programos viešai prieinamų sertifikatų duomenų bazėje https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/search ar lygiavertėje;	*Sertifikato numeris ir nuoroda: #2658* https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2658 *Rubrik turi CMVP (Cryptographic Module Validation Program) sertifikatą, kuris patvirtina jo kriptografinių modulių atitiktį FIPS 140-2 standartams. Šis sertifikatas užtikrina, kad Rubrik naudojamos kriptografinės funkcijos atitinka duomenų apsaugos saugumo reikalavimus.* *Rubrik Cryptographic Library suteikia FIPS 140-2 standarto validuotas kriptografines funkcijas, įskaitant AES, RSA, ECDSA ir HMAC algoritmus. Šis sertifikavimas galioja, kai sistema veikia FIPS režimu (FIPS mode), užtikrindama atitiktį saugumo standartams.*
2.9.2.	kiekvieno telkinio mazgai vienas į kitą turi autentifikuotis sertifikatais. Komunikacijoms tarp mazgų turi būti naudojamas ne prastesnis nei TLSv1.2 ar lygiavertis transporto saugos protokolas;	*Rubrik užtikrina saugią mazgų (nodes) autentifikaciją naudodama Transport Layer Security (TLS) protokolą. Veikimo principai:* *• Certificate-Based Mutual Authentication: Rubrik klasteriai (clusters) naudoja TLS sertifikatus mazgų autentifikavimui ir užšifruotam ryšiui užtikrinti.*

		• TLS 1.2 for Internal Communications: visa vidinė komunikacija tarp mazgų (intra-node) ir tarp klasterių (inter-cluster) apsaugota naudojant TLS 1.2 protokolą, tuo tarpu išorinės aplikacijos gali naudoti TLS 1.1, jei jos nepalaiko TLS 1.2. *• Data Encryption in Transit: visi duomenys, perduodami tarp mazgų, yra užšifruojami naudojant TLS, taip užkertant kelią neleistinam priėjimui, net ir duomenų perėmimo atveju.* *• TLS Certificate Management: Rubrik teikia TLS sertifikatų valdymo priemones (management workflow), leidžiančias administratoriams importuoti, redaguoti ir šalinti sertifikatus pagal poreikį.* *Šios saugumo priemonės užtikrina duomenų konfidencialumą, vientisumą (integrity) ir patikimą autentifikavimą Rubrik klasteriuose.*
2.9.3.	telkiniai privalo palaikyti KMIP protokolą ir ne žemesnę nei 1.4 jo versiją (ar lygiavertį), ir turi būti suderinamas su perkančiosios organizacijos turima išorine Thales CipherTrust Manager 2.x versijos raktų saugykla. Turi būti pateikta nuoroda į oficialią gamintojo svetainę arba turi būti pateiktas gamintojo ar jo atstovo raštas laisva forma, kad telkiniai yra suderinami su nurodyta išorinių raktų saugykla;	*Pateikiamas gamintojo atstovo raštas, patvirtinantis, kad telkiniai yra suderinami su išorine Thales CipherTrust Manager 2.x versijos raktų saugykla.* *Rubrik palaiko KMIP (Key Management Interoperability Protocol) protokolą, skirtą išorinių raktų valdymo tarnybų (Key Management Services – KMS) integracijai.* *Kalbant apie Thales CipherTrust Manager versiją 2.x, Thales pateikia integravimo žingsnius, kaip konfigūruoti KMIP serverius su CipherTrust Manager. Tai apima:* *• CA sertifikatų (CA certificates) įkėlimą,* *• KMIP serverio nustatymų (server settings) konfigūravimą,* *• Užtikrinimą, kad AES raktai (AES keys) būtų generuojami CipherTrust Manager serveryje.*
2.9.4.	telkiniai turi naudoti nekeičiamą (angl. *immutable*) failų sistemą, t.y. turi neleisti keisti išsaugotų duomenų. Telkinių naudojamos failų sistemos turi būti apsaugotos nuo trečiųjų šalių kenkimo programų įdiegimo;	*Rubrik užtikrina duomenų nekintamumą (immutability), siekiant apsaugoti atsarginių kopijų (backup) duomenis nuo išpirkos reikalaujančių virusų (ransomware) ir neautorizuotų pakeitimų. Šis mechanizmas veikia taip:* *• Immutable File System (Atlas): Rubrik naudojama Atlas failų sistema neleidžia daryti jokių pakeitimų saugomuose atsarginių kopijų duomenyse, užtikrindama, kad kartą įrašyti duomenys negali būti keičiami ar ištrinami (Append Only Filesystem).*

		• Zero-Trust Architecture: Veiksmus galima atlikti tik naudojant autentifikuotas API sąsajas (authenticated APIs), tokiu būdu užkertant kelią neautorizuotam priėjimui. *• Ransomware Protection: Kadangi duomenys negali būti perrašomi, net užkrėsti failai negali plisti pačioje atsarginių kopijų sistemoje.* *• Air-Gapped Backups: Rubrik palaiko loginį atsarginių kopijų atskyrimą (logical air-gapping), kuris užtikrina, kad atsarginės kopijos liktų izoliuotos nuo gamybinės aplinkos.* *• Retention Lock: Administratoriai gali taikyti saugojimo politiką (retention policies), kuri užtikrina, kad atsarginės kopijos nebūtų ištrintos anksčiau nustatyto termino.* *Integruotas „Rubrik“ duomenų nekintamumas (immutability) užtikrina duomenų vientisumą (data integrity) ir atsparumą kibernetinėms grėsmėms (cyber resilience).*
2.9.5.	telkiniai turi naudoti technologiją, matuojančią laiko tėkmę (angl. *passage of time*) ir neturi būti priklausomi nuo NTP serverio laiko (ar lygiaverčio). Reikalui esant atsarginės kopijos išlaikymo laiko pakeitimas turi būti patvirtinamas ne mažiau kaip dviejų įrenginį administruojančių darbuotojų;	*Rubrik užtikrina tikslų laiko sinchronizavimą naudodamas Monotonic Clock funkciją ir NTP apsaugą:* *Rubrik naudoja monotonic clock – paskirstytą laiko sinchronizavimo tarnybą, skirtą vienodam laiko sinchronizavimui tarp visų mazgų (nodes). Tai užtikrina:* *• Nuoseklias laiko žymas (timestamps) atsarginių kopijų (backup) ir atkūrimo (recovery) operacijoms.* *• Atsparumą gedimams dėl laikrodžio poslinkių (clock skew) ir staigių sisteminio laiko šuolių (system time jumps).* *• Klasterio lygio sinchronizaciją, neleidžiančią įvykių tvarkos nesuderinamumui.* *Rubrik palaiko saugią NTP konfigūraciją, kad būtų išvengta kenkėjiškų sistemos laiko keitimų. Pagrindinės saugumo priemonės apima:* *• Šifruotą NTP autentifikaciją (encrypted NTP authentication) laiko šaltiniams patikrinti.* *• Apsaugą nuo laiko klastojimo atakų (time spoofing attacks), užtikrinančią tikslų sinchronizavimą.* *• Klasterio mastu taikomus NTP nustatymus, leidžiančius administratoriams užtikrinti saugią laiko sinchronizaciją.*

		Šios funkcijos užtikrina patikimą laiko stebėjimą, taip išvengiant trikdžių atsarginių kopijų kūrimo ir atkūrimo procesuose. *Rubrik Quorum Authentication (dar žinoma kaip Quorum Authorization) yra saugumo funkcija, reikalaujanti kelių asmenų patvirtinimo prieš vykdant kritinius veiksmus Rubrik Security Cloud (RSC) aplinkoje. Tai užtikrina, kad nė vienas vartotojas negali modifikuoti ar ištrinti apsaugotų duomenų be papildomo patvirtinimo.* *Pagrindinės Quorum Authentication savybės:* *• Multi-User Approval: Kritiniams duomenims įtakos turintys veiksmai reikalauja patvirtinimo iš paskirtų QAuth peržiūrėtojų (reviewers) prieš juos vykdant.* *• Policy-Based Protection: Administratoriai gali apibrėžti quorum authorization politiką, nurodydami patvirtinimo reikalavimus konkrečioms operacijoms.* *• Role-Based Access Control (RBAC):* *• QAuth Admin: valdo quorum authorization nustatymus ir politikas.* *• QAuth Reviewer: patvirtina arba atmeta apsaugotus veiksmus.* *• Requester: inicijuoja veiksmus, kuriems reikalingas patvirtinimas.* *• Protection Against Unauthorized Changes: Užkerta kelią atsitiktiniams arba kenkėjiškiems atsarginių kopijų konfigūracijų ir saugumo nustatymų pakeitimams.* *• Automation Exclusion: Tarnybinės paskyros (service accounts) gali būti išimtos iš quorum authorization politikų, siekiant išvengti trikdžių automatizuotuose procesuose.* *Šios priemonės užtikrina papildomą saugumo lygmenį, užkertantį kelią neteisėtiems arba atsitiktiniams svarbių duomenų pakeitimams „Rubrik“ sistemoje.*
2.9.6.	telkiniai privalo aptikti ir pranešti apie anomalijas – įvykus kenkimo ir išpirkos reikalaujančių programų (angl. *ransomware*) atakai turi gebėti identifikuoti kurie duomenys	*Rubrik anomalijų aptikimo funkcionalumas (Anomaly Detection) leidžia proaktyviai aptikti įtartiną veiklą atsarginių kopijų (backup) duomenyse*

	buvo paveikti, kurios atsarginės kopijos yra nepažeistos, kurios atsarginės kopijos buvo atliktos prieš ataką, taip suteikiant galimybę greitai atkurti duomenis iki nepažeistos būklės momento. Telkiniai turi turėti galimybę atlikti anomalijų analizę tiesiogiai atsarginėse kopijose, nereikalaujant jų nukopijuoti ar prijungti kitur. Turi būti pateikti visi komponentai ir visos licencijos šiam funkcionalumui įgalinti (jei tokie reikalingi);	*– nereikia papildomai kopijuoti ar prijungti kitur duomenų iš klasterio (cluster):* *• Machine Learning-Based Analysis: Rubrik naudoja iš anksto apmokytus didžiuosius kalbos modelius (Large Language Models – LLMs), kad atskirtų teisėtus duomenų pakeitimus nuo potencialių grėsmių.* *• Behavioral Monitoring: sistema analizuoja failų sistemos (file system) statistiką, siekdama aptikti neįprastus veiklos šablonus (patterns), tokius kaip masiniai duomenų ištrynimai (mass deletions), modifikacijos (modifications) arba užšifravimai (encryptions). Tai leidžia nustatyti, kurios atsarginės kopijos yra nepažeistos, kurios atsarginės kopijos buvo atliktos prieš ataką, taip suteikiant galimybę greitai atkurti duomenis iki nepažeistos būklės momento. Funkcionalumas įeina į siūlomą bazinę licenciją.*
2.10.	**Tinklas:** kiekvienas mazgas turi turėti ne mažiau nei du prievadus, kurie palaikytų ne mažesnę nei 25 Gbps spartą programinei įrangai valdyti ir duomenų srautams užtikrinti. Šie prievadai turi palaikyti 802.3ad (angl. *LACP - Link Aggregation Control Protocol*), 802.1q (angl. *VLAN Tagging*) ar lygiavertes technologijas bei turi būti suderinami su perkančiosios organizacijos turimais Cisco Nexus komutatoriais. Papildomai turi būti bent vienas ne mažesnės nei 1 Gbps spartos tam numatytas prievadas aparatūrinės dalies valdymui ir stebėjimui. Į pasiūlymą turi būti įtraukti visi komponentai (rekomenduojami SFP28 moduliai, ne trumpesni nei 3 metrų kabeliai ir kt.) pilnai dubliuotam pajungimui į aukščiau minimus komutatorius;	*Kiekvienas R7408 mazgas turi keturis prievadus, kurie palaiko 25 Gbps spartą programinei įrangai valdyti ir duomenų srautams užtikrinti. Šie prievadai palaikyti 802.3ad (angl. LACP - Link Aggregation Control Protocol), 802.1q (angl. VLAN Tagging) bei yra suderinami su perkančiosios organizacijos turimais Cisco Nexus komutatoriais. Papildomai kiekviename R7408 mazge yra vienas 1 Gbps spartos tam numatytas prievadas aparatūrinės dalies valdymui ir stebėjimui.* *Į pasiūlymą įtraukti SFP28 moduliai ir 3 metrų kabeliai pilnai dubliuotam pajungimui į Cisco Nexus komutatorius.*
2.11.	**Suderinamumas su trečiųjų šalių produktais:** telkiniai turi integruotis į perkančiosios organizacijos turimas VMware vSphere 8.x ir 7.x ar lygiavertes virtualizuotas aplinkas ir turi būti pilnai su jomis suderinamos. Telkiniai privalo palaikyti VADP (angl. *VMware vStorage APIs for Data Protection*) ar lygiavertę technologiją. Telkiniai turi galėti atskirti atsarginių kopijų ir valdymo tinklo srautus kai šios	*Rubrik telkiniai integruojasi į perkančiosios organizacijos turimas VMware vSphere 8.x ir 7.x virtualizuotas aplinkas ir yra pilnai su jomis suderinami. Telkiniai palaiko VADP (angl. VMware vStorage APIs for Data Protection) technologiją. Telkiniai gali atskirti atsarginių kopijų ir valdymo tinklo srautus kai šios galimybės yra prieinamos. Telkiniai išnaudoja pasikeitusių duomenų sekimo mechanizmą (angl. CBT – Changed Block Tracking). Telkiniai gali sukurti atsargines virtualių*

	galimybės yra prieinamos. Telkiniai privalo išnaudoti pasikeitusių duomenų sekimo ar lygiavertį mechanizmą (angl. *CBT – Changed Block Tracking*). Telkiniai privalo sukurti atsargines virtualių mašinų kopijas bei gebėti atstatyti virtualias mašinas į tas pačias ar kitas perkančiosios organizacijos turimas VMware vSphere virtualizuotas aplinkas. Atsarginėse kopijose esančius virtualios mašinos duomenis (bylą ar aplanką su visu jo turiniu) turi būti galima atstatyti į tą pačią, kitą ar visiškai naują virtualią mašiną. Momentinės duomenų nuotraukos (angl. *snapshot*) vientisumas turi būti palaikomas Microsoft Exchange Server, Microsoft SQL Server, Microsoft Active Directory, Microsoft SharePoint ir Oracle Database (RDBMS) ar lygiavertėms, veikiančioms Windows Server ar lygiavertėse operacinėse sistemose. Turi būti palaikomas Oracle RMAN ar lygiavertis įrankis rezervinių kopijų sukūrimui ir atstatymui. Papildomai turi būti palaikomas augimo sujungimo (angl. *incremental Merge*) funkcionalumas**. Kartu su pasiūlymu turi būti pateikta nuoroda į oficialią gamintojo dokumentaciją arba turi būti pateiktas gamintojo ar jo atstovo raštas laisva forma, patvirtinantis suderinamumą su perkančiosios organizacijos aukščiau minimais trečiųjų šalių produktais;**	*mašinų kopijas bei geba atstatyti virtualias mašinas į tas pačias ar kitas perkančiosios organizacijos turimas VMware vSphere virtualizuotas aplinkas. Atsarginėse kopijose esančius virtualios mašinos duomenis (bylą ar aplanką su visu jo turiniu) galima atstatyti į tą pačią, kitą ar visiškai naują virtualią mašiną. Momentinės duomenų nuotraukos (angl. snapshot) vientisumas yra palaikomas Microsoft Exchange Server, Microsoft SQL Server, Microsoft Active Directory, Microsoft SharePoint ir Oracle Database (RDBMS), veikiančioms Windows Server operacinėse sistemose. Palaikomas Oracle RMAN įrankis rezervinių kopijų sukūrimui ir atstatymui. Papildomai yra palaikomas augimo sujungimo (angl. incremental Merge) funkcionalumas. Kartu su pasiūlymu pateikiama oficiali gamintojo suderinamumo matrica ir Rubrik CDM vartotojo gidas, patvirtinantys suderinamumą su perkančiosios organizacijos aukščiau minimais trečiųjų šalių produktais;*
2.12.	**Valdymas:** telkinių valdymo sąsaja turi būti realizuota 3 skirtingais būdais: • Komandine eilute (per SSH ar lygiavertį protokolą); • Grafiniu (per naršyklę). Turi būti naudojama HTML 5 ar lygiavertė technologija, kitos technologijos negalimos. Turi būti palaikomos populiariausios naršyklės – Google Chrome, Mozilla Firefox, Microsoft Edge ar lygiavertės. Turi būti galimybė įsidiegti lokalizuotą sertifikatą; • Programiniu (angl. *API – Application Programming Interface*); Telkiniai turi būti pilnai valdomi kiekvienu iš šių valdymo būdų. Kiekvienas iš valdymo būdų turi gebėti valdyti visus telkinio	*Rubrik telkinių valdymo sąsaja yra realizuota 3 skirtingais būdais:* *• Komandine eilute (per SSH ar lygiavertį protokolą);* *• Grafiniu (per naršyklę). Naudojama HTML 5 technologija. Palaikomos populiariausios naršyklės – Google Chrome, Mozilla Firefox, Microsoft Edge. Yra galimybė įsidiegti lokalizuotą sertifikatą;* *• Programiniu (angl. API – Application Programming Interface);* *Telkiniai yra pilnai valdomi kiekvienu iš šių valdymo būdų. Kiekvienas iš valdymo būdų geba valdyti visus telkinio mazgus. Valdymo funkcionalumas užtikrinamas jei lieka veikti bent vienas mazgas. Programinė įranga geba užduotis paskirstyti visiems mazgams. Visi valdymo būdai geba konfigūruoti ataskaitų teikimą pagal turimą talpą, naudojamą talpą, naudojamą talpą po duomenų glaudinimo, dienos,*

	mazgus. Valdymo funkcionalumas turi būti užtikrinamas jei lieka veikti bent vienas mazgas. Programinė įranga turi gebėti užduotis paskirstyti visiems mazgams. Visi valdymo būdai turi gebėti konfigūruoti ataskaitų teikimą pagal turimą talpą, naudojamą talpą, naudojamą talpą po duomenų glaudinimo, dienos, savaitės, mėnesio sunaudotos talpos pokyčius, talpos ateities prognozavimą (angl. *forecast*) ar pagal kitus gamintojo siūlomus parametrus;	*savaitės, mėnesio sunaudotos talpos pokyčius, talpos ateities prognozavimą (angl. forecast);* *Rubrik Security Cloud (RSC)valdymo priemonė (Control Plane)* *• Centralized Management: RSC veikia kaip vieninga valdymo konsolė (single pane of glass), leidžianti administratoriams centralizuotai valdyti duomenų apsaugos politikas (data protection policies), saugumo nustatymus ir atkūrimo operacijas įvairiuose darbo krūviuose (workloads).* *• Zero Trust Security: RSC taiko vaidmenų pagrindu veikiančią prieigos kontrolę (role-based access control – RBAC) ir daugiapakopį autentifikavimą (multi-factor authentication – MFA), užtikrinant saugią prieigą.* *• Automated Threat Detection: naudodama mašininį mokymąsi (machine learning), RSC nuolat stebi duomenis ir identifikuoja anomalijas, taip aptikdama išpirkos reikalaujančių programų (ransomware) atakas ir neautorizuotus duomenų pakeitimus.* *• Immutable Backups: RSC užtikrina atsarginių kopijų nekintamumą (immutability), apsaugodama nuo duomenų sugadinimo ar ištrynimo.* *• Kubernetes Protection: RSC veikia kaip Kubernetes duomenų apsaugos valdymo priemonė, valdydama „Persistent Volume“ atsargines kopijas (backups) Rubrik klasteryje.* *• Cloud-Native Architecture: RSC, sukurta naudojant „Google Cloud Platform“ (GCP), remiasi mikroservisų (microservices) architektūra, užtikrinančia didelį mastelį ir aukštą pasiekiamumą (high availability).* *RSC suteikia kibernetinį atsparumą (cyber resilience), užtikrindama, kad perkančioji organizacija gali efektyviai apsaugoti, stebėti ir atkurti savo duomenis.* *RSC API architektūra ir integracija* *RSC yra pagrįsta API (API-first) architektūra, leidžiančia sklandžiai integruoti ją į įmonės sistemas ir automatizacijos procesus. Veikimo principai:*

		API galimybės RSC sistemoje: *• GraphQL ir REST API: RSC palaiko tiek GraphQL, tiek REST API, leidžiančias lankstų duomenų užklausų vykdymą ir automatizavimą.* *• Pre-Built Integrations: RSC turi iš anksto sukurtas integracijas su tokiomis įmonių sistemomis kaip „ServiceNow“, „Terraform“, „VMware Cloud Director“ ir kitais įrankiais.* *• Self-Service Automation: Organizacijos gali automatizuoti atsarginių kopijų kūrimą (backup), atkūrimą (recovery) ir saugumo operacijas naudodamos „Rubrik“ API SDK bibliotekas, skirtas „Python“, „Go“ ir „PowerShell“.* *• Centralized Monitoring: RSC API integruojamos su „Splunk“, „Prometheus“ ir „Nagios“ sistemomis, užtikrinant realaus laiko stebėseną (real-time observability).* *API Playground* *Rubrik suteikia „API Playground“ – interaktyvią kūrimo aplinką, kurioje vartotojai gali:* *• Naršyti ir išbandyti GraphQL API užklausas (queries).* *• Patvirtinti API operacijas prieš įdiegiant automatizavimo scenarijus (scripts).* *• Valdyti API autentifikaciją ir prieigos kontrolę (access control).* *Rubrik klasteris taip pat suteikia komandinės eilutės sąsają (command-line interface – CLI), leidžiančią atlikti sudėtingesnes konfigūracijas ir diagnostiką Rubrik klasteriuose bei Rubrik Edge virtualiuose įrenginiuose (virtual appliances).*
2.13.	**Autentifikavimasis ir rolės:** telkiniai turi palaikyti autentifikavimą, grupes ir vartotojus iš Microsoft Active Directory, LDAP ar lygiaverčių sistemų. Telkiniuose turi būti palaikomas kelių faktorių autentifikavimasis (angl. *MFA – Multi-Factor Authentication*). Telkiniai turi palaikyti vienkartinius slaptažodžius (angl. *TOTP – Time-based One-Time Password*). Telkiniai turi palaikyti RBAC (angl. *Role Based Access Control*) ar lygiavertę privilegijų sistemą – turi palaikyti administratoriaus,	*Rubrik telkiniai palaiko autentifikavimą, grupes ir vartotojus iš Microsoft Active Directory, LDAP sistemų.* *Rubrik naudoja pažangius autentifikavimo mechanizmus, kad apsaugotų naudotojų paskyras ir sistemos prieigą:* *• Multi-Factor Authentication (MFA): Palaiko Time-Based One-Time Password (TOTP) tipo MFA tiek vietinėms (local), tiek LDAP paskyroms.* *• Single Sign-On (SSO): Integruojama su SAML 2.0 Identity Providers (IdP), tokiais kaip Okta, Duo ir Ping Identity.*

	operatoriaus, auditoriaus ir kitas gamintojo standartiškai įdiegtas roles;	• *Strong Password Enforcement: Aptinkami brutalaus prisijungimo bandymai (brute-force attacks) ir blokuojami naudotojai su kompromituotais slaptažodžiais.* • *Two-Step Verification: Administratoriai gali taikyti privalomą MFA politiką, kad sustiprintų prieigos saugumą.* • *IP Allowlisting: Prisijungimo prieiga apribojama tam tikrais IP adresais, kas padeda apsaugoti nuo neleistinų prisijungimų.* *Rubrik užtikrina saugią prieigos kontrolę naudodama Role-Based Access Control (RBAC), RBAC riboja prieigą pagal naudotojo rolę (user role), užtikrindama, kad tik įgalioti asmenys galėtų atlikti konkrečius veiksmus.* *Pagrindinės funkcijos:* • *Predefined Roles: „Rubrik" pateikia iš anksto apibrėžtas roles, tokias kaip Administrator, Read-Only Admin ir Infrastructure Admin, kurioms suteikti konkretūs leidimai.* • *Custom Roles: Administratoriai gali kurti individualias (custom) roles, pritaikytas pagal organizacijos poreikius.* • *Least Privilege Enforcement: Naudotojai gauna tik tiek teisių, kiek būtina jų užduotims atlikti, taip sumažinant saugumo rizikas.* • *Separation of Duties: Skirtingos rolės leidžia paskirstyti atsakomybes, todėl jautrioms operacijoms gali būti reikalaujamas kelių asmenų patvirtinimas, kas apsaugo nuo neleistinų pakeitimų.* *Šios saugumo priemonės užtikrina tvirtą prieigos kontrolę ir apsaugo Rubrik klasterius nuo neautorizuotos prieigos bei kibernetinių grėsmių.*
2.14.	**Duomenų sinchronizavimas:** telkiniai turi gebėti sinchronizuoti duomenis vienas į kitą naudojant tiek vienos krypties sinchronizacijos tipą (angl. *one-way replication*), tiek dvikryptį sinchronizacijos tipą (angl. *bi-directional replication)*. Telkiniai turi gebėti šifruoti tarpusavio komunikacinius ryšius duomenų sinchronizavimo procedūrai atlikti ne prastesniu nei TLSv1.2 ar lygiaverčiu transporto saugos protokolu. Jei duomenų sinchronizacijos funkcijai atrakinti reikalinga licencija, ji turi būti pateikta kiekvienam telkiniui. Jei ši funkcija licencijuojama per duomenų kiekius,	*Duomenų sinchronizavimas ir replikacija* • *One-Way & Bi-Directional Replication: Rubrik palaiko tiek vienkryptę, tiek dvikryptę replikaciją, leidžiančią klasteriams vienu metu siųsti ir gauti duomenis.* • *SLA-Based Replication: Administratoriai gali apibrėžti replikacijos politikas SLA domenų (SLA Domains) lygiu, taip užtikrinant efektyvų duomenų sinchronizavimą.* • *Multi-Cluster Replication: Vienas Rubrik klasteris gali replikuoti duomenis į kelis kitus klasterius, palaikydamas many-to-one, many-to-many ir one-to-one replikacijos modelius.* *Duomenų sinchronizavimo šifravimas*

	licencijos turi būti pateiktos kiekvieno telkinio visai siūlomai naudingai talpai;	*• TLS 1.2 Encryption: Rubrik šifruoja visus perduodamus duomenis (data in flight) naudodama TLS 1.2, taip užtikrindama saugų perdavimą tarp klasterių.* *• AES-256 Encryption: Duomenys, saugomi klasteryje (data at rest), yra apsaugoti naudojant AES-256 šifravimą, atitinkantį saugumo reikalavimus.* *• KMIP Support: Rubrik integruojasi su KMIP protokolą palaikančiomis išorinėmis raktų valdymo sistemomis (key managers), leidžiančiomis centralizuotai valdyti šifravimo raktus.* *Duomenų sinchronizacijos funkcijai atrakinti atskira licencija nereikalinga.*
2.15.	**Automatizavimas ir integracija su išorinėmis sistemomis, kitos papildomos savybės:**	
2.15.1.	telkiniai turi turėti integraciją su Splunk, Ansible ar lygiavertėmis sistemomis;	*Rubrik integruojasi su Splunk, Ansible ir kitais įmonės automatizavimo bei stebėsenos įrankiais, siekiant pagerinti sistemų stebimumą (observability), saugumą ir operacinį efektyvumą.* *Rubrik pateikia Splunk Add-on, leidžiantį organizacijoms:* *• Vizualizuoti veikimo būseną naudodami prietaisų skydus (dashboards).* *• Stebėti saugumo įvykius, įskaitant išpirkos reikalaujančių programų (ransomware) aptikimą ir audito žurnalus (audit logs).* *• Stebėti atsarginių kopijų darbų (backup job) sėkmės ir nesėkmės dažnius, kad būtų galima laiku identifikuoti problemas.* *• Analizuoti talpos naudojimo tendencijas (capacity trends) keliuose Rubrik klasteriuose.* *Rubrik siūlo Ansible modulius, skirtus automatizuoti tiekimo procesus (provisioning), konfigūracijos valdymą (configuration management) ir atsarginių kopijų operacijas:* *• Automatizuotas SLA priskyrimas darbo krūviams (workloads).* *• Momentinių kopijų (snapshot) kūrimas pagal poreikį virtualioms mašinoms (VMs).* *• Live Mount automatizavimas greitam atkūrimui.* *• Infrastructure-as-Code (IaC) palaikymas, leidžiantis lengvai įdiegti sprendimus infrastruktūroje kaip kodą.*

		Rubrik palaiko API pagrįstas integracijas su įvairiais įmonės įrankiais, įskaitant: *• ServiceNow – IT paslaugų valdymui (ITSM).* *• Terraform – infrastruktūros automatizavimui.* *• Nagios ir Prometheus – centralizuotai stebėsenai.* *• VMware Cloud Director –debesų duomenų apsaugai (cloud-native data protection).* *Rubrik API-first architektūra užtikrina sklandų suderinamumą su trečiųjų šalių platformomis, leidžiančiais organizacijoms automatizuoti darbo procesus, sustiprinti saugumą ir optimizuoti duomenų apsaugos procesus.*
2.15.2.	telkiniuose turi būti galimybė automatizuoti procesus naudojant PowerShell, Python ar lygiavertes programavimo aplinkas;	*Rubrik suteikia plačias automatizavimo galimybes per PowerShell, Python ir REST API.* *PowerShell automatizavimas* *• Rubrik PowerShell Module: Rubrik siūlo specialų PowerShell SDK, leidžiantį administratoriams automatizuoti tokius veiksmus kaip:* *• Atsarginių kopijų politikų (backup policy) taikymą tarp skirtingų klasterių.* *• Live Mount ir Instant Recovery operacijas.* *• Ataskaitų ir audito žurnalų (reporting & audit log) paėmimą atitikties užtikrinimui.* *• Secure Authentication: PowerShell scenarijai autentifikuojami naudojant API tokens, užtikrinant saugų komandų vykdymą.* *Python automatizavimas* *• Rubrik Python SDK: oficialus Rubrik Python SDK leidžia automatizuoti atsarginių kopijų darbo eigas (backup workflows), debesijos integracijas (cloud integrations) ir ataskaitas.* *• Infrastructure-as-Code (IaC) support: organizacijos gali naudoti Python skriptus SLA Domains valdymui, replikacijos politikų konfigūravimui ir ransomware detection darbo eigos inicijavimui.* *• Event-Driven Automation: Python leidžia integraciją su Ansible, Terraform ir ServiceNow, automatizuojant saugumo atsakus ir atsarginių kopijų politikas.*

		Kitos palaikomos programavimo aplinkos *• REST API & GraphQL: Rubrik pateikia API galinius taškus (endpoints), leidžiančius tiesiogiai sąveikauti su sistema ir vykdyti automatizaciją skirtingose platformose.* *• Ansible Playbooks: iš anksto paruošti Ansible moduliai leidžia automatizuoti infrastruktūrą tiek debesijos, tiek vietinėje (on-prem) aplinkoje.* *• Terraform Provider for Rubrik: leidžia naudoti Infrastructure-as-Code (IaC) metodą programiškai valdant Rubrik klasterius.* *Rubrik taikomas API-first principas užtikrina, kad administratoriai gali efektyviai automatizuoti ir integruoti atsarginių kopijų kūrimo, atkūrimo ir saugumo procesus įmonės turimose aplinkose.*
2.15.3.	telkiniai turi gebėti automatiškai įtraukti naujas virtualias mašinas ir duomenų bazes į esamą rezervinio kopijavimo aplinką pagal nustatytas politikas (angl. *policy-based automation*);	*Rubrik telkiniai geba automatiškai įtraukti naujas virtualias mašinas ir duomenų bazes į esamą rezervinio kopijavimo aplinką pagal nustatytas politikas ir suteikia automatizuotą, politikomis grįstą objektų (workloads) apsaugą.* *Kaip veikia politikomis pagrįsta automatizacija* *• SLA Domains: Rubrik leidžia administratoriams apibrėžti Service Level Agreement (SLA) Domains, kurie automatiškai įgyvendina atsarginių kopijų (backup), replikacijos (replication) ir saugojimo laikotarpių (retention) politikas.* *• Hierarchical Protection: SLA Domains gali būti taikomi skirtinguose hierarchijos lygiuose, leidžiant automatizuotai priskirti apsaugą naujai atsiradusiems objektams (pvz. VM, DB).* *• Tag-Based Assignments: darbo krūviai gali būti apsaugoti automatiškai pagal metaduomenų žymas (metadata tags), užtikrinant dinamišką politikų taikymą.* *• Cross-Region Replication: SLA Domains palaiko automatinę momentinių kopijų (snapshot) replikaciją tarp skirtingų regionų, taip užtikrinant pasirengimą nelaimėms (disaster recovery).* *Šis funkcionalumas leidžia Rubrik automatiškai taikyti duomenų apsaugos strategijas organizacijos mastu, sumažinant rankinį administravimą ir padidinant saugumo bei atkūrimo efektyvumą.*

2.15.4.	telkiniuose turi būti galimybė automatizuoti rezervinio kopijavimo procesų eiles ir tvarkaraščius pagal iš anksto numatytą aprašą. Turi būti suteikta galimybė naudoti tą patį aprašą keliems skirtingiems objektams bei aplinkoms;	*Rubrik telkiniuose yra galimybė automatizuoti rezervinio kopijavimo procesų eiles ir tvarkaraščius pagal iš anksto numatytą aprašą. Yra galimybė naudoti tą patį aprašą keliems skirtingiems objektams bei aplinkoms.* *Rubrik Global SLA Domains suteikia vieningą požiūrį į duomenų apsaugos politikų valdymą įvairiems objektams (workloads) ir aplinkoms. Jos supaprastina atsarginių kopijų tvarkaraščius, saugojimo laikotarpius (retention), replikaciją ir archyvavimą, taikydamos automatizuotą politikų valdymą.* *Pagrindinės Rubrik Global SLA Domains savybės:* *• Centralized Policy Management: Administratoriai gali apibrėžti SLA Domains, kurie taikomi keliems darbo krūviams ir/ar klasteriams (clusters), užtikrinant nuoseklią apsaugą.* *• Automated Backup Scheduling: Darbo krūviai automatiškai apsaugomi pagal iš anksto nustatytas politikas, taip pašalinant poreikį rankiniu būdu planuoti atsarginių kopijų tvarkaraščius.* *• Replication & Archival: SLA Domains palaiko replikaciją tarp klasterių (cross-cluster replication) ir ilgalaikį duomenų archyvavimą į debesijos (cloud) arba vietinius (on-premises) saugojimo sprendimus.* *• Retention Lock: Suteikia governance ir compliance režimus, kurie apsaugo duomenis nuo neautorizuoto ištrynimo, atitinkant reguliacinius reikalavimus.* *• Legal Hold for Snapshots: Administratoriai gali taikyti teisinius sulaikymus (legal hold) momentinėms kopijoms (snapshots), neleisdami jų ištrinti anksčiau laiko.*
2.15.5.	telkiniuose rezervinės kopijos turi būti indeksuojamos greitai paieškai atlikti. Jei rezervinės kopijos yra perkeliamos į kitus saugojimo įrenginius (2.15.10 p.), jos taipogi turėtų būti indeksuojamos;	*Rubrik indeksavimo mechanizmas klasteriuose ir archyvuose užtikrina efektyvų duomenų paieškos ir atkūrimo procesą visose momentinėse kopijose (snapshots).* *Indeksavimas Rubrik klasteriuose* *• File Indexing for Snapshots: Rubrik leidžia failų indeksavimą (file indexing) apsaugotiems objektams (workloads), suteikdama galimybę administratoriams ieškoti duomenų per indeksuotas momentines kopijas greitam atkūrimui.*

		• Metadata Management: sistema palaiko kiekvienos momentinės kopijos metaduomenis (metadata), užtikrindama greitą duomenų paiešką ir prieigą. *• Automated Indexing: indeksavimas automatiškai įjungiamas tam tikriems darbo krūviams, pvz., Azure virtual machines, siekiant užtikrinti greitą atkūrimą.* *Indeksavimas archyvuose* *• Archival Snapshot Indexing: archyvuojant duomenis, Rubrik nustato, ar įkelti tik pakitusią momentinės kopijos dalį (incremental), ar pilną kopiją (full copy).* *• Metadata Preparation: prieš archyvavimą Rubrik paruošia metaduomenis, kad užtikrintų efektyvų indeksavimą ir vėlesnę prieigą prie duomenų.* *• Encrypted Index Storage: indeksavimo failai saugiai laikomi archyvuose, naudojant šifravimą (encrypted index storage), taip užtikrinant duomenų vientisumą ir atitiktį reikalavimams (compliance).* *Rubrik indeksavimo galimybės pagerina paieškos galimybes, atkūrimo greitį ir archyvavimo efektyvumą.*
2.15.6.	telkinių agentų instaliavimas bei atnaujinimas turi nereikalauti serverių perkrovimo;	*Rubrik telkinių agentų - Rubrik Backup Service (RBS) diegimui bei atnaujinimui nereikia sistemos perkrovimo, nes jie sukurti taip, kad būtų galima sklandžiai įdiegti Windows, Linux ir Unix sistemose be trikdžių vykstančioms operacijoms:* *• Agent-Based Deployment: RBS įdiegiama kaip „lengvas“ agentas (lightweight agent), kuris nesikiša į sistemai kritinius procesus.* *• Non-Intrusive Installation: Diegimo metu nėra modifikuojami branduolio lygmens komponentai (kernel-level components), todėl nereikia sistemos paleidimo iš naujo.* *• Automated Configuration: Įdiegus, RBS automatiškai prisiregistruoja prie Rubrik cluster iš karto tampa pasiekiamais.* *• Push Installation Support: Administratoriai gali diegti RBS į kelias sistemas vienu metu naudodami automatizavimo įrankius, tokius kaip Puppet ar Chef.*

2.15.7.	perkančiosios organizacijos turimoms virtualizuotoms aplinkoms turi būti palaikomas amžinai augantis (*angl. incremental forever*) rezervinio kopijavimo būdas, užtikrinant kopijavimo tęstinumą net kai virtuali mašina perkeliama iš vieno perkančiosios organizacijos turimo VMware vCenter į kitą;	*Rubrik Atlas failų sistema palaiko incremental forever tipo atsargines kopijas, užtikrinant optimalų saugyklų panaudojimą ir greitą duomenų atkūrimą.* *Kaip Atlas veikia su Incremental Forever backups:* *• Versioned File Storage: kiekvieną virtualios mašinos (VM) momentinę kopiją (snapshot) traktuoja kaip versijuotą failą (versioned file), saugodama tik skirtumus (delta changes) tarp momentinių kopijų.* *• Snapshot Chain Integrity: pirmoji momentinė kopija yra pilna kopija, o vėlesnės momentinės kopijos saugo tik pakitimus (incremental changes). Atlas užtikrina, kad senesnės momentinės kopijos išliktų validžios ir tinkamos duomenų atkūrimui.* *• Replica Placement: užuot atsitiktinai paskirsčiusi duomenų blokus (data blocks), Atlas susijusius duomenis talpina tuose pačiuose konkrečiuose mazguose (nodes), taip padidinant efektyvumą ir našumą.* *• Archival Consolidation: kai momentinių kopijų saugojimo laikas baigiasi, Atlas konsoliduoja duomenis iš pasibaigusių momentinių kopijų į naujesnes, taip sumažindama nereikalingą vietos panaudojimą.* *• Data Striping: Atlas paskirsto (stripes) duomenis tarp kelių diskų mazgo (node) viduje, taip užtikrindama greitesnius skaitymo/rašymo procesus ir didesnį atsparumą gedimams (fault tolerance).* *• Flash Optimization: dažnai naudojami duomenys laikomi flash tipo atmintinėse, užtikrinant greitą jų prieigą ir sumažinant vėlavimą (latency).*
2.15.8.	kai vienas atsarginio kopijavimo telkinys yra sunaikintas, turi būti galimybė atstatyti duomenis iš kopijos, laikomos kitame nutolusiame telkinyje. Kopija turi turėti savyje visą informaciją, reikalingą tokiam duomenų atkūrimui;	*Sunaikinus vieną atsarginio kopijavimo telkinį yra galimybė atstatyti duomenis iš kopijos, kuriamos automatinės replikacijos būdu ir laikomos kitame nutolusiame telkinyje. Kopija savyje turi visą informaciją (metaduomenis, indeksus, konfigūracijos duomenis), reikalingą tokiam duomenų atkūrimui, t.y. replikuojamos atsarginės kopijos yra pilnavertės ir savarankiškos.*
2.15.9.	telkiniai turi gebėti aptikti grėsmes naudojant arba YARA, arba SIGMA, arba lygiavertes taisykles;	*Rubrik Threat Hunting funkcionalumas (reikalinga Enterprise Edition License) leidžia aktyviai aptikti ir reaguoti į kibernetines grėsmes, analizuojant atsarginių kopijų (backups) duomenis pagal*

		kompromitacijos indikacijas (Indicators of Compromise – IOCs). Funkcionalumo veikimo principas: *Rubrik Threat Hunting* *• IOC-Based Scanning: Rubrik skenuoja atsargines kopijas pagal žinomus failų maišos kodus (file hashes), failų šablonus (file patterns) ir YARA taisykles, kad aptiktų kenkėjiškas programas arba įtartiną veiklą.* *• Turbo Threat Hunting: ši funkcija leidžia itin greitai skenuoti iki 75 000 atsarginių kopijų per 60 sekundžių, padedant nustatyti švarius atkūrimo taškus (recovery points).* *• Historical Analysis: Rubrik analizuoja momentines kopijas (snapshots) per ilgesnį laikotarpį, nustatydamas, kada įvyko pirminis užkrėtimas, ir taip užkirsdamas kelią pakartotiniam užsikrėtimui (reinfection).* *• Automated Threat Hunt: administratoriai gali nustatyti reguliarius arba pagal poreikį (on-demand) vykdomus skenavimus, kurie leidžia aptikti duomenų anomalijas atsarginėse kopijose.* *YARA taisyklės Rubrik sistemoje:* *• Pattern-Based Detection: YARA taisyklės leidžia Rubrik sistemai aptikti kenkėjiškas programas, lyginant konkrečius dvejetainius (binary) ar tekstinius (textual) failų šablonus (patterns).* *• Custom Rule Creation: saugumo specialistai gali sukurti individualias (custom) YARA taisykles naujai atsirandančioms grėsmėms aptikti.* *• Integration with Threat Intelligence: Rubrik naudoja iš anksto sugeneruotus maišos kodus (precomputed hash values) ir YARA taisykles, siekiant padidinti kenkėjiškų programų aptikimo efektyvumą.* *Rubrik Threat Hunting ir YARA taisyklių integracija suteikia aktyvią kibernetinės saugos apsaugą, užtikrinančią, kad perkančioji organizacija galėtų efektyviai aptikti ir atkurti duomenis po kibernetinių incidentų.*
2.15.10.	telkiniai turi palaikyti archyvą (angl. *long term archive*). Telkiniai turi gebėti perkelti archyvą ir jose laikomas rezervines	*Rubrik suteikia duomenų archyvo perkėlimą į debesį (Cloud), Amazon S3 ir NFS, užtikrindamas efektyvų ilgalaikį duomenų saugojimą ir atkūrimą.*

	kopijas į kitus saugojimo įrenginius naudojant NFS ar lygiavertį protokolą. Telkiniai turi gebėti nukopijuoti rezervinę kopiją į archyvą ar atstatyti kopiją iš archyvo naudojant perkančiosios organizacijos turimą NetApp FAS8200 saugyklą. Turi būti naudojamos standartinės sąsajos nediegiant jokios papildomos programinės įrangos. Rezervinių kopijų atstatymas iš archyvo turi būti valdomas per tą pačią vartotojo sąsają kaip ir kiti atstatymai;	*Rubrik klasteriai archyvuoja duomenis remdamiesi archyvavimo politikomis (archival policies), kurios apibrėžia:* *• Archyvavimo vietas (Cloud, Local S3, NFS, juostų įrenginius naudojant QStar Archive Manager).* *• Archyvuotų momentinių kopijų (snapshots) saugojimo laikotarpius (retention periods).* *• Šifravimo (encryption) ir glaudinimo (compression) nustatymus saugiam saugojimui.* *Rubrik palaiko NFS archyvą, leidžiantį organizacijoms saugoti atsargines kopijas (backups) tinklo prijungtoje saugykloje (Network Attached Storage – NAS):* *• Palaikomas dalinis (inkrementinis) arba pilnas momentinių kopijų (snapshots) įkėlimas pagal archyvavimo politikas.* *• Programinis šifravimas (software encryption) NFS įrenginiams, kurie nepalaiko vidinio šifravimo (native encryption).* *• Archyvų konsolidavimas (archival consolidation), siekiant atlaisvinti saugojimo vietą.*
2.16.	**Maitinimo šaltiniai:** bet kokia siūloma fizinė įranga turi turėti ne mažiau nei 2 vienas kitą dubliuojančius maitinimo šaltinius. Fizinė įranga turi gebėti balansuoti elektros naudojimą per visus maitinimo šaltinius. Įranga turi gebėti veikti tik su vienu maitinimo šaltiniu. Turi būti pasiūlyti ne mažiau kaip 2 metrų ir ne daugiau kaip 3 metrų ilgio maitinimo kabeliai. Siūlomos techninės įrangos maitinimo įtampa turi būti 230V 50Hz, o maitinimo kabeliai turi būti pateikiami su Lietuvos Respublikoje naudojamomis jungtimis į elektros tinklą (IEC-60320 arba C13/C14, arba C19/C20, arba lygiavertėmis);	*Siūloma fizinė įranga turi 2 vienas kitą dubliuojančius maitinimo šaltinius. Fizinė įranga geba balansuoti elektros naudojimą per abu maitinimo šaltinius. Įranga geba veikti tik su vienu maitinimo šaltiniu. Komplekte pateikiami 2 metrų ilgio maitinimo kabeliai. Siūlomos techninės įrangos maitinimo įtampa yra 230V 50Hz, o maitinimo kabeliai yra su Lietuvos Respublikoje naudojamomis C13/C14 jungtimis į elektros tinklą;*
2.17.	**Aplinkos veiksniai:** telkiniai turi veikti nuo 10 iki 35 laipsnių pagal Celsijų aplinkos temperatūroje ir nuo 8% iki 90% santykinėje oro drėgmėje be rasos taško kondensacijos. Telkinius turi būti galima saugoti nuo	*Telkiniai veikia nuo 10 iki 35 laipsnių pagal Celsijų aplinkos temperatūroje ir nuo 8% iki 90% santykinėje oro drėgmėje be rasos taško kondensacijos. Telkinius galima saugoti nuo -10 iki 60 laipsnių temperatūroje pagal Celsijų ir nuo 5% iki 95% santykinėje oro drėgmėje be rasos taško kondensacijos.*

	-10 iki 60 laipsnių temperatūroje pagal Celsijų ir nuo 5% iki 95% santykinėje oro drėgmėje be rasos taško kondensacijos;	
2.18.	**Kiti reikalavimai:** kartu su fizine įranga turi būti pateikti visi įrangos įdiegimui reikalingi kabeliai bei montavimo priedai;	
2.19.	**Garantinis aptarnavimas:** siūlomai techninei ir programinei įrangai turi būti suteikta ne mažiau nei 60 mėnesių gamintojo užtikrinta garantija ją aptarnaujant perkančiosios organizacijos patalpose įrangos eksploatavimo vietoje be jokių papildomų mokesčių. Techninis palaikymas turi būti teikiamas 24 valandas per parą, 7 dienas per savaitę, 365 dienas per metus viso garantinio laikotarpio metu. Pranešimus apie gedimus turi priimti: • gamintojas savo techninio palaikymo interneto svetainėje; • gamintojas telefonu arba elektroniniu paštu; arba • Tiekėjas telefonu arba elektroniniu paštu; Nurodyti galimus pranešimų apie gedimus pateikimo būdus. Reakcijos laikas į pranešimus apie tai, kad: • sistema neveikia (aukšto kritiškumo) - ne ilgesnis nei 30 minučių; • sumažėjęs sistemos funkcionalumas (vidutinio kritiškumo) - ne ilgesnis nei 2 valandos; • pastebėti smulkūs gedimai arba norint užduoti bendro pobūdžio klausimus (žemo kritiškumo) - ne ilgesnis nei kita darbo diena; Programinės įrangos atnaujinimai ir saugumo pataisymai turi būti teikiami be jokių papildomų mokesčių viso garantinio laikotarpio metu. Gamintojas turi turėti viešai prieinamą interneto svetainę, iš kurios būtų galima atsisiųsti sistemos dokumentaciją, mikrokodo (angl. *firmware*) ar programinės įrangos atnaujinimus, saugumo pataisymus, taip pat turi būti galima pasitikrinti informaciją apie garantijos galiojimą. Tiekėjas turi garantuoti nemokamą dalių tiekimą siūlomai	*Siūlomas gamintojo techninio aptarnavimo planas - PREMIUM SUPPORT SERVICES PLAN 60 mėn. trukmės, taip pat komplektuojama opcija - Non-Returnable Disk Service for Rubrik R7000 Appliance, užtikrinanti, kad sugedus magnetiniams ar puslaidininkiniams diskams, jų nereikia grąžinti ir pirkėjas juos gali sunaikinti perkančiosios organizacijos patalpose.* *Siūlomas gamintojo techninio aptarnavimo planas užtikrina, kad siūlomai techninei ir programinei įrangai suteikiama 60 mėnesių gamintojo užtikrinta garantija techninę įrangą aptarnaujant perkančiosios organizacijos patalpose įrangos eksploatavimo vietoje be jokių papildomų mokesčių. Techninis palaikymas teikiamas 24 valandas per parą, 7 dienas per savaitę, 365 dienas per metus viso garantinio laikotarpio metu. Pranešimus apie gedimus gamintojas priima:* • *gamintojas savo techninio palaikymo interneto svetainėje;* • *gamintojas telefonu ir elektroniniu paštu;* • *per Rubrik CDM UI;* *Reakcijos laikas į pranešimus apie tai, kad:* • *sistema neveikia (aukšto kritiškumo) 30 - minučių;* • *sumažėjęs sistemos funkcionalumas (vidutinio kritiškumo) - 2 valandos;* • *smulkūs gedimai – 8 valandos* • *užduodant bendro pobūdžio klausimus (žemo kritiškumo) - kita darbo diena;* *Programinės įrangos atnaujinimai ir saugumo pataisymai teikiami be jokių papildomų mokesčių viso garantinio laikotarpio metu. Gamintojas turi viešai prieinamą interneto svetainę (apsaugotą vartotojo vardu ir slaptažodžiu bei dinamiškai generuojamu vienkartiniu slaptažodžiu), iš kurios galima atsisiųsti sistemos dokumentaciją, mikrokodo (angl. firmware) bei programinės įrangos atnaujinimus, saugumo pataisymus, taip pat galima pasitikrinti informaciją apie garantijos galiojimą.*

	sistemai ir nemokamus remonto darbus garantiniu laikotarpiu. Pakaitinės detalės turi būti pristatytos ir pakeistos ne vėliau kaip per 3 darbo dienas. Garantinio laikotarpio metu sugedus magnetiniams ar puslaidininkiniams diskams, jie nėra grąžinami, o sunaikinami perkančiosios organizacijos patalpose. Garantiniu laikotarpiu neremontuotinai sugedusi įranga turi būti pakeista ekvivalenčia nauja, sąlygas ir terminus derinant su perkančiąja organizacija;	*Tiekėjas per gamintojo servisą garantuoja nemokamą dalių tiekimą siūlomai sistemai ir nemokamus remonto darbus garantiniu laikotarpiu. Pakaitinės detalės pristatomos ir pakeičiamos per 3 darbo dienas (dalys išsiunčiamos tą pačią darbo dieną, kai diagnozuojamas gedimas). Garantinio laikotarpio metu sugedus magnetiniams ar puslaidininkiniams diskams, jie nėra grąžinami, o sunaikinami perkančiosios organizacijos patalpose. Garantiniu laikotarpiu neremontuotinai sugedusi įranga bus pakeista ekvivalenčia nauja, sąlygas ir terminus derinant su perkančiąja organizacija;*
2.20.	**Įrangos pristatymas:** įranga turi būti pristatyta į NKSC techninį centrą, adresu: Verslo Centras 349, 8 aukštas, Savanorių pr. 349, 51480, Kaunas	
2.21.	**Diegimo darbai:** diegimo darbus turi atlikti gamintojo, jo atstovo arba Tiekėjo paskirtas programinės įrangos specialistas. Perkančioji organizacija negali sudaryti sąlygų diegimo darbus atlikti įrangos nuolatinio eksploatavimo vietoje, todėl pirminis įrangos konfigūravimas turės būti atliekamas NKSC techninio centro patalpose. Gamintojo, jo atstovo arba Tiekėjo paskirtas programinės įrangos specialistas įrangos pirminio konfigūravimo metu turės paruošti ir perkančiajai organizacijai perduoti komutavimo schemas ir visą reikalingą dokumentaciją įrenginių sukomutavimui nuolatinio eksploatavimo vietoje. Perkančioji organizacija fizinę įrangą išveš į nuolatinio eksploatavimo vietą ir komutuos savo jėgomis griežtai laikantis gamintojo arba Tiekėjo paskirto programinės įrangos specialisto nurodytų instrukcijų. Perkančioji organizacija, ne vėliau kaip per 5 darbo dienas atlikusi fizinės įrangos montavimą ir komutavimą, gamintojo, jo atstovo arba Tiekėjo paskirtam programinės įrangos specialistui suteiks nuotolinę prieigą sistemos būklės patikrinimui ir tolesniems diegimo darbams atlikti. Diegimo darbai bus laikomi atliktais, kai siūloma atsarginių kopijų sistema padaro bent vienos virtualios mašinos bent vieną atsarginę kopiją iš perkančiosios organizacijos turimų virtualizuotų aplinkų atskiriant atsarginių kopijų tinklo srautą nuo valdymo srauto, sėkmingai suveikia duomenų sinchronizavimo funkcija ir atsarginė kopija atstatoma kitoje virtualizuotoje aplinkoje traktuojant, kad pirminis telkinys yra sunaikintas. Perkančioji organizacija papildomai pageidauja, kad atsarginių kopijų sistemos diegimo darbai apimtų integraciją su archyvams skirtomis erdvėmis (2.15.10 p.) bei duomenų užšifravimu (2.9.3 p.). Perkančioji organizacija turimus integruojamus įrenginius konfigūruos savo jėgomis padedant už diegimo darbus atsakingam programinės įrangos specialistui. Įvedimo į eksploataciją (diegimo) paslauga turi būti įskaičiuota į pasiūlymo kainą;	
2.22.	**Mokymai:** gamintojas arba Tiekėjas turi pravesti ne mažiau kaip 4 dienų kursus, kurie skirti perkančiosios organizacijos 2 darbuotojams. Kurso tikslas – supažindinti perkančiosios organizacijos darbuotojus su siūlomos sistemos darbo pradžiamoksliu ir baziniais pagrindais. Kursai turi būti nuotoliniai. Mokymai turi būti organizuojami Lietuvos laiko zonoje nuo pirmadienio iki penktadienio darbo dienos metu išskyrus švenčių dienas. Perkančiosios organizacijos darbuotojų apmokymai turi būti įskaičiuoti į pasiūlymo kainą;	
2.23.	**Įrangos pristatymo, diegimo darbų ir Perkančiosios organizacijos darbuotojų apmokymų terminai:** 90 kalendorinių dienų nuo Sutarties įsigaliojimo dienos;	

Jeigu techninėje specifikacijoje ir (ar) kituose pridedamuose dokumentuose apibūdinant pirkimo objektą nurodytas konkretus pavadinimas ar šaltinis, konkretus procesas ar prekės ženklas, patentas, tipai, konkreti kilmė ar gamyba, standartas, Tiekėjas gali pateikti lygiavertį sprendinį (kitų gamintojų lygiavertė produkcija ar įranga, pan.) nurodytajam. Lygiavertiškumo įrodymas yra Tiekėjo pareiga.