KONKURSO DOKUMENTŲ
2 priedas

PREKIŲ TIEKIMO TECHNINĖ SPECIFIKACIJA

1. KONKURSO objektas yra PREKIŲ TIEKIMAS. TIEKĖJAS turi būti oficialus siūlomų PREKIŲ gamintojo atstovas, įgaliotas parduoti siūlomas PREKES.

Techniniai reikalavimai pagal kiekvieną KONKURSO objekto dalį

2. **<u>KONKURSO OBJEKTO 1 DALIS — Programinės įrangos konteinerių valdymo sistema ir virtualios platformos funkcionalumo plėtra.</u>**

Eil. Nr.	Parametras	Reikalaujama reikšmė	Atitikimas
Reikalavimai programinės įrangos konteinerių valdymo sistemai:			
1.	Gamintojas, modelio pavadinimas	Nurodyti gamintoją, modelio pavadinimą, įrangos kodą.	Gamintojas: VMware Modelis: Upgrade: VMware NSX Data Center Professional to NSX Data Center Advanced per Processor Kodas: NX-DC-PFADV-UG-C 3 metų palaikymas: VMware Support and Subscription Production - technical support - for VMware NSX Data Center Advanced - 3 year Kodas: 3 x NX-DC-ADV-P-SSS-C Modelis: VMware TANZU STANDARD TERM SUBSCRIPTION + PRODUCTION SUPPORT FOR 3 YEAR (PER CPU). Kodas: TNZ-STD-CPU-TLSS-3Y-C Modelis: VMware Pivotal LabsTM Navigator – 4wks Kodas: SVC-1247
2.	Licencijų paskirtis	Sistemos licencija turi užtikrinti konteinerio kaip paslauga CaaS (angl. Container as a Service) funkciją.	Sistemos licencija užtikrina konteinerio kaip paslauga CaaS (angl. Container as a Service) funkciją.
3.	Reikalavimai licencijavimui	Licencijos turi palaikyti ne mažiau kaip 16 (šešiolika) vnt. fizinių procesorių. Branduolių skaičius neturi būti ribojamas. Licencijos neturi riboti virtualių mašinų skaičiaus. Turi būti galimybė didinti palaikomų tarnybinių stočių ir procesorių skaičių įsigyjant papildomas licencijas. Licencijos galiojimas ne mažiau kaip 36 mėn.	Licencijos palaiko 16 (šešiolika) vnt. fizinių procesorių. Branduolių skaičius neribojamas. Licencijos neriboja virtualių mašinų skaičiaus. Yra galimybė didinti palaikomų tarnybinių stočių ir procesorių skaičių, įsigyjant papildomas licencijas. Licencijos galiojimas 36 mėn.
4.	Reikalavimai valdymo sąsajai	- turi turėti valdymo naudotojo sąsają (UI), į kurią įeina intuityvi	- turi valdymo naudotojo sąsają (UI), į kurią įeina intuityvi GUI,

		GUI, kad naudotojas galėtų naudotis veiksmingai ir efektyviai; - turi leisti valdymo naudotojo sąsajai rasti informaciją apie virtualius įrenginius, konfigūravimo parinktis ir naujausių įvykių santrauką; - turi suteikti naudotojui galimybę pridėti arba ištrinti konteinerius per valdymo naudotojo sąsają; - turi leisti naudotojams prijungti nuotolinę konsolę prie tam tikrų talpyklų, kad būtų galima praktiškai valdyti svečių (angl. Guest) operacinę sistemą per valdymo naudotojo sąsają; - naudotojo sąsaja turi leisti keisti sudėtinių rodinių konfigūracijas; - naudotojo sąsaja turi leisti valdyti naudotojus ir jų grupes; - valdymo naudotojo sąsaja turi leisti naudotojams konfigūruoti užsakovo eksploatuojamas vSAN tipo saugyklas; - valdymo sąsaja turi leisti naudotojams sukonfigūruoti ESX serverį (tik “root” naudotojams); - turi būti galimybė išorinėms sistemoms apeiti naudotojo sąsają ir tiesiogiai naudoti API, neprarandant funkcionalumo ir saugumo; - sistema turi turėti komandų eilutės sąsają (CLI); - valdymo naudotojo sąsaja turi būti pasiekiama per visas šiuolaikines interneto naršykles; - valdymo naudotojo sąsaja turi gebėti valdyti virtualizacijos tinklo elementus; - turi būti galimybė balansuoti apkrovas tarp konteinerių per naudotojo sąsaja.	kad naudotojas galėtų naudotis veiksmingai ir efektyviai; - leidžiama valdymo naudotojo sąsajai rasti informaciją apie virtualius įrenginius, konfigūravimo parinktis ir naujausių įvykių santrauką; - suteikiama naudotojui galimybė pridėti arba ištrinti konteinerius per valdymo naudotojo sąsają; - leidžiama naudotojams prijungti nuotolinę konsolę prie tam tikrų talpyklų, kad būtų galima praktiškai valdyti svečių (angl. Guest) operacinę sistemą per valdymo naudotojo sąsają; - naudotojo sąsaja leidžia keisti sudėtinių rodinių konfigūracijas; - naudotojo sąsaja leidžia valdyti naudotojus ir jų grupes; - valdymo naudotojo sąsaja leidžia naudotojams konfigūruoti užsakovo eksploatuojamas vSAN tipo saugyklas; - valdymo sąsaja leidžia naudotojams sukonfigūruoti ESX serverį (tik “root” naudotojams); - yra galimybė išorinėms sistemoms apeiti naudotojo sąsają ir tiesiogiai naudoti API, neprarandant funkcionalumo ir saugumo; - sistema turi komandų eilutės sąsają (CLI); - valdymo naudotojo sąsaja yra pasiekiama per visas šiuolaikines interneto naršykles; - valdymo naudotojo sąsaja geba valdyti virtualizacijos tinklo elementus; - yra galimybė balansuoti apkrovas tarp konteinerių per naudotojo sąsaja.
5.	Reikalavimai paslaugų (angl. Service) aptikimui ir registravimui	- turi užtikrinti dinamišką paslaugų (angl. Services) aptikimą ir komunikaciją tarp aptiktų paslaugų; - turi užtikrinti paslaugų (angl. Services) registravimą, kad konteineriai galėtų tinkamai pranešti apie savo būseną	- užtikrinamas dinamiškas paslaugų (angl. Services) aptikimas ir komunikacija tarp aptiktų paslaugų; - užtikrinamas paslaugų (angl. Services) registravimas, kad konteineriai galėtų tinkamai pranešti apie savo būseną

		paslaugų aptikimo sluoksniu (angl. Service Discovery Layer); - turi turėti būsenos stebėjimo komponentą, kuris patikrina ar konteineris yra pasiekiamas ir atnaujintas; - turi suteikti naudotojams galimybę peržiūrėti pagrindines paslaugų matricas ir stebėti konteinerių paslaugas; - turi suteikti naudotojams galimybę nustatyti paslaugų tipą, teikiamą kiekvienoje VM (Virtual Machine) aplinkoje; - turi leisti naudotojams stebėti, kuri VM yra naudojama kaip paslaugos dalis bei koks VM išjungimo ar perkėlimo poveikį sistemai; - turi suteikti naudotojams galimybę nustatyti, kurios VM naudojamos paslaugai perkelti ir kurioms paslaugoms gali turėti įtakos VM ar kito infrastruktūros komponento praradimas; - turi leisti prieigą prie VM svečio (angl. Guest) operacinės sistemos teisėmis (angl. Credentials).	paslaugų aptikimo sluoksniu (angl. Service Discovery Layer); - yra būsenos stebėjimo komponentas, kuris patikrina ar konteineris yra pasiekiamas ir atnaujintas; - suteikiama naudotojams galimybė peržiūrėti pagrindines paslaugų matricas ir stebėti konteinerių paslaugas; - suteikiama naudotojams galimybė nustatyti paslaugų tipą, teikiamą kiekvienoje VM (Virtual Machine) aplinkoje; - leidžiama naudotojams stebėti, kuri VM yra naudojama kaip paslaugos dalis bei koks VM išjungimo ar perkėlimo poveikis sistemai; - suteikia naudotojams galimybę nustatyti, kurios VM naudojamos paslaugai perkelti ir kurioms paslaugoms gali turėti įtakos VM ar kito infrastruktūros komponento praradimas; - leidžiama prieiga prie VM svečio (angl. Guest) operacinės sistemos teisėmis (angl. Credentials).
6.	Reikalavimai paslaugų (angl. service) katalogui	- turi turėti paslaugų katalogą, kuriame atvaizduojamos programos ir paslaugos esančios klasteryje; - turi leisti naudoti CI/CD (angl. „Continuous integration / Continuous delivery“) automatizavimą, leidžianti įdiegti paslaugas ir konfigūruoti darbo krūvius bei priklausomybes; - privalo turėti registrus, kurie naudojami konteinerio atvaizdams laikyti; - turi leisti naršyti paslaugų katalogą naudojant sistemos savitarnos portalu; - turi leisti paslaugų architektams ir administratoriams sukurti naujas paslaugas ir paskelbti jas bendrajame kataloge; - turi leisti naudotojų grupėms ar administratoriams nurodyti	- Turi paslaugų katalogą, kuriame atvaizduojamos programos ir paslaugos esančios klasteryje; - leidžiama naudoti CI/CD (angl. „Continuous integration / Continuous delivery“) automatizavimą, leidžiantį įdiegti paslaugas ir konfigūruoti darbo krūvius bei priklausomybes; - turi registrus, kurie naudojami konteinerio atvaizdams laikyti; - leidžiama naršyti paslaugų kataloge naudojant sistemos savitarnos portalu; - leidžiama paslaugų architektams ir administratoriams sukurti naujas paslaugas ir paskelbti jas bendrajame kataloge; - leidžiama naudotojų grupėms ar administratoriams nurodyti politikas, pvz., Kas turi teisę reikalauti konkrečių katalogo elementų arba atlikti konkrečius

		politikas, pvz., Kas turi teisę reikalauti konkrečių katalogo elementų arba atlikti konkrečius veiksmus su teikiamais elementais.	veiksmus su teikiamais elementais.
7.	Reikalavimai įeinančių paslaugų maršrutizavimui (angl. Ingress Service Routing)	- turi turėti įeinančių paslaugų mašrutizavimo funkcionalumą, kuris automatizuoja naujų programų URL paskelbimą išorėje, įskaitant paslaugos užklausos vidinį susiejimą ir maršrutizavimą iki konteinerio; - turi leisti pateikti HTTP arba HTTPS maršrutus iš klasterio išorės į vieną ar daugiau vidinio klasterio paslaugų; - turi leisti „Kubernetes“ klasteriams palaikyti patekimą per trečiųjų šalių valdiklius, tokius kaip „Contour“ ir „Nginx“; - turi suteikti naudotojams galimybę pateikti įeinančių paslaugų mašrutizavimo specifikacijas, kuriose yra visa informacija, reikalinga apkrovos balansavimui arba tarpiniam (angl. Proxy) serveriui konfigūruoti.	- yra įeinančių paslaugų mašrutizavimo funkcionalumas, kuris automatizuoja naujų programų URL paskelbimą išorėje, įskaitant paslaugos užklausos vidinį susiejimą ir maršrutizavimą iki konteinerio; - leidžiama pateikti HTTP arba HTTPS maršrutus iš klasterio išorės į vieną ar daugiau vidinio klasterio paslaugų; - leidžiama „Kubernetes“ klasteriams palaikyti patekimą per trečiųjų šalių valdiklius, tokius kaip „Contour“ ir „Nginx“; - suteikiama naudotojams galimybė pateikti įeinančių paslaugų mašrutizavimo specifikacijas, kuriose yra visa informacija, reikalinga apkrovos balansavimui arba tarpiniam (angl. Proxy) serveriui konfigūruoti.
8.	Reikalavimai paslaugų tinklui (angl. Service Mesh)	- turi turėti paslaugų tinklo funkcionalumą, kuris įgalina ir kontroliuoja ryšį tarp paslaugų; - turi turėti orkestravimo ir planavimo funkcionalumą; - paslaugų tinklas turi leisti vaidmenimis (angl. Role-based access control) ir atributais (angl. Attribute-based access control) pagrįstą prieigos valdymą; - paslaugų tinklas turi leist RPC (angl. Remote procedure call) lygio autorizaciją; - paslaugų tinklas turi suteikti galimybę valdyti įeinančius ir išeinančius srautus ir leisti naudotojams pritaikyti stebėjimo ir maršrutizavimo taisykles; - turi leisti apjungti skirtingus paslaugų tinklus veikiančius skirtinguose klasteriuose ir skirtingose infrastuktūrose; - turi leisti atskirti duomenų srautą 7-ajame OSI (angl. Open Systems	- yra paslaugų tinklo funkcionalumas, kuris įgalina ir kontroliuoja ryšį tarp paslaugų; - yra orkestravimo ir planavimo funkcionalumas; - paslaugų tinklas leidžia vaidmenimis (angl. Role-based access control) ir atributais (angl. Attribute-based access control) pagrįstą prieigos valdymą; - paslaugų tinklas leidžia RPC (angl. Remote procedure call) lygio autorizaciją; - paslaugų tinklas suteikia galimybę valdyti įeinančius ir išeinančius srautus ir esant poreikiui naudotojams pritaikyti stebėjimo ir maršrutizavimo taisykles; - leidžiama apjungti skirtingus paslaugų tinklus veikiančius skirtinguose klasteriuose ir skirtingose infrastuktūrose; - leidžiama atskirti duomenų srautą 7-ajame OSI (angl. Open

		Interconnection model) taikomųjų aplikacijų lygyje.	Systems Interconnection model) taikomųjų aplikacijų lygyje.
9.	Reikalavimai programinės įrangos plečiamumui	- turi turėti išplėtimo sluoksnį, kuris suteikia sąsają valdymui ir tvarkaraščių sudarymui; - valdymo įrankis turi turėti darbo eigos dizainerį, kuris leistu kurti darbo eigas “drag and drop” principu; - valdymo įrankis darbo eigos ir papildinių įrankiai turi suteikti naudotojams galimybę lengvai atlikti tokias užduotis: priskirti IP adresą iš IP adresų valdymo įrankio, sugeneruoti darbo užsakymo užduotį, atnaujinti konfigūracijos valdymo duomenų bazę, konfigūruoti apkrovos balansavimą, inicijuoti sistemos atsargines kopijas; - valdymo įrankis turi palaikyti skriptų programavimo kalbas, įskaitant „PowerShell“, „Node.js“ ir „Python“; - valdymo įrankis turi turėti REST API; - Sistema turi palaikyti CNI (angl. Container Network Interface), CRI (angl. Container Runtime Interface) ir CSI (angl. Container Storage Interface) „Kubernetes“ sąsajas.	- yra išplėtimo sluoksnis, kuris suteikia sąsają valdymui ir tvarkaraščių sudarymui; - valdymo įrankis turintis darbo eigos dizainerį, kuris leidžia kurti darbo eigas “drag and drop” principu; - valdymo įrankis darbo eigos ir papildinių įrankiai suteikia naudotojams galimybę lengvai atlikti tokias užduotis: priskirti IP adresą iš IP adresų valdymo įrankio, sugeneruoti darbo užsakymo užduotį, atnaujinti konfigūracijos valdymo duomenų bazę, konfigūruoti apkrovos balansavimą, inicijuoti sistemos atsargines kopijas; - valdymo įrankis palaiko skriptų programavimo kalbas, įskaitant „PowerShell“, „Node.js“ ir „Python“; - valdymo įrankis turi REST API; - Sistema palaiko CNI (angl. Container Network Interface), CRI (angl. Container Runtime Interface) ir CSI (angl. Container Storage Interface) „Kubernetes“ sąsajas.
10.	Reikalavimai konteinerių vykdymo laikui (angl. Container Runtime)	- turi sudaryti sąlygas konteinerio vykdymui ir klasterio mazgams suteikti galimybę gauti registre esančius konteinerio vaizdus; - turi sudaryti sąlygas konteinerio vykdymui ir suteikti tinkamai failų struktūrai paleisti konteinerį pagrindiniame serveryje (angl. Host); - turi leisti administratoriams valdyti darbo krūvius naudojant konteinerio vykdymo laiką; - turi sudaryti sąlygas konteinerio vykdymui ir sąveikauti su tinklo ir saugyklos papildiniais; - turi suteikti galimybę kurti, paleisti ir sustabdyti konteinerių vykdymą;	- sudarytos sąlygos konteinerio vykdymui ir klasterio mazgams suteikiama galimybė gauti registre esančius konteinerio vaizdus; - sudarytos sąlygos konteinerio vykdymui ir suteikiama galimybė tinkamai failų struktūrai paleisti konteinerį pagrindiniame serveryje (angl. Host); - leidžia administratoriams valdyti darbo krūvius naudojant konteinerio vykdymo laiką; - sudarytos sąlygos konteinerio vykdymui ir sąveikavimui su tinklo ir saugyklos papildiniais; - suteikta galimybė kurti, paleisti ir sustabdyti konteinerių vykdymą;

		- Sistema turi būti pilnai suderinama su OCI konteinerių vykdymo formatu.	- Sistema yra pilnai suderinama su OCI konteinerių vykdymo formatu.
11.	Reikalavimai stebėsenos funkcionalumui	- turi leisti stebėti konteinerius veikimo metu (angl. runtime) ir pagrindinį serverį (angl. host) branduolio lygyje (angl. kernel-level); - turi turėti stebėjimo komponentą kuris leistų matyti klasterio mazgus, konteinerius, mirko procesus veikimo metu (angl. runtime); - turi turėti galimybę atvaizduoti sukauptus resursų našumo duomenis (procesoriaus, atminties, saugyklos ir t.t.) grafine forma (grafikai, diagramos ir t.t.); - komandinės eilutės pagalba turi leisti naudotojui detaliai analizuoti sistemos našumo parametrus; - turi liesti greitai identifikuoti darbingus ir problemas patiriančius serverius; - turi liesti konfigūruoti sistemos stebėsenos veiksmus po atsiradusių įvykių, įspėjimų ir aliarmų; - turi kaupti sistemos įvykius stebėjimo žurnale; - turi kaupti papildomus įvykius apie veiklą virtualizavimo platformos aplinkoje; - turi liesti administratoriui atlikti šiuos veiksmus: stebėti sistemos darbingumą serverio aparatūriniame lygyje, stebėti sistemos darbingumą virtualizavimo lygyje; konfigūruoti „alarm“ tipo pranešimus; konfigūruoti SNMP žinutes, šalinti trikius sistemoje; - turi liesti stebėti šiuos parametrus: pasiekiamumą, našumą, apkrautumą, įvykius, pakeitimus visuose virtualizacijos sluoksniuose. - turi turėti vieningą grafinę naudotojo sąsają, kurios pagalba būtų galima valdyti ir konfigūruoti visus infrastuktūros ir taikomųjų programų serverius	- leidžiama stebėti konteinerius veikimo metu (angl. runtime) ir pagrindinį serverį (angl. host) branduolio lygyje (angl. kernel-level); - esantis stebėjimo komponentas leidžia matyti klasterio mazgus, konteinerius, mikro procesus veikimo metu (angl. runtime); - suteikta galimybė atvaizduoti sukauptus resursų našumo duomenis (procesoriaus, atminties, saugyklos ir t.t.) grafine forma (grafikai, diagramos ir t.t.); - komandinės eilutės pagalba galima naudotojui detaliai analizuoti sistemos našumo parametrus; - leidžiama greitai identifikuoti darbingus ir problemas patiriančius serverius; - leidžiama konfigūruoti sistemos stebėsenos veiksmus po atsiradusių įvykių, įspėjimų ir aliarmų; - kaupiami sistemos įvykiai stebėjimo žurnale; - kaupiami papildomi įvykiai apie veiklą virtualizavimo platformos aplinkoje; - leidžiama administratoriui atlikti šiuos veiksmus: stebėti sistemos darbingumą serverio aparatūriniame lygyje, stebėti sistemos darbingumą virtualizavimo lygyje; konfigūruoti „alarm“ tipo pranešimus; konfigūruoti SNMP žinutes, šalinti trikdžius sistemoje; - leidžiama stebėti šiuos parametrus: pasiekiamumą, našumą, apkrautumą, įvykius, pakeitimus visuose virtualizacijos sluoksniuose. - turima vieninga grafinė naudotojo sąsaja, kurios pagalba galima valdyti ir konfigūruoti visus infrastuktūros ir taikomųjų programų serverius (angl.

		(angl. middleware) bei aplikacijų stebėjimo sistemos komponentus.	middleware) bei aplikacijų stebėjimo sistemos komponentus.
12.	Reikalavimai programinės įrangos saugumo funkcionalumui	- turi turėti galimybę integruoti konteinerių apsaugos priemones (pvz. WAF, IDS); - Sistemos registrai turi naudoti rolėmis pagrįsta prieigos valdymo kontrolė (angl. Role Based Access Control - RBAC); - Konteinerių orchestravimo sistema turi būti kontroliuojama rolėmis pagrįsta prieigos valdymo kontrolė (angl. Role Based Access Control - RBAC); - turi užtikrinti kad aplikacijų kopijos (angl. „images“) ir konteineriai būtų apsaugoti nuo neautorizuoto modifikavimo; - turi užtikrinti, kad aplikacijų kopijos (angl. „images“) ir konteineriai būtų audituojami; - turi užtikrinti, kad aplikacijų kopijos iš išorinių šaltinių prieš paleidimą būtų ištestuotos ir akredituotos; - turi būti galimybę uždrausti neakredituotų aplikacijų kopijų (angl. „images“) paleidimą; - be papildomų priemonių ar licencijų turi turėti integracijos su Užsakovo turima aktyvaus katalogo sistema (MS ActiveDirectory) galimybę, naudotojų autentifikavimui ir autorizavimui; - sistemos konteinerių saugumo ir stebėsenos įrankiai turi turėti galimybę integruotis su saugumo stebėsenos įvykių valdymo (SIEM) įrankiais; - konteineriams turi būti uždrausta prisijungti prie pagrindinės (angl. „Host“) tarnybines stoties direktorijų. (pvz. System32, "etc", bin); - aplikacijų kopijų (angl. „images“) pažeidžiamumas turi būti tikrinamas kūrimo metu, o aplikacijų kopijos esančios registre tikrinamos kasdien; - sistema turi palaikyti duomenų šifravimą (angl. encryption at rest);	- yra galimybė integruoti konteinerių apsaugos priemones (pvz. WAF, IDS); - Sistemos registrai naudojami rolėmis pagrįsta prieigos valdymo kontrole (angl. Role Based Access Control - RBAC); - Konteinerių orchestravimo sistema yra kontroliuojama rolėmis pagrįsta prieigos valdymo kontrole (angl. Role Based Access Control - RBAC); - yra užtikrinama kad aplikacijų kopijos (angl. „images“) ir konteineriai būtų apsaugoti nuo neautorizuoto modifikavimo; - yra užtikrinama, kad aplikacijų kopijos (angl. „images“) ir konteineriai būtų audituojami; - yra užtikrinama, kad aplikacijų kopijos iš išorinių šaltinių prieš paleidimą būtų ištestuotos ir akredituotos; - yra galimybė uždrausti neakredituotų aplikacijų kopijų (angl. „images“) paleidimą; - be papildomų priemonių ar licencijų yra integracijos su Užsakovo turima aktyvaus katalogo sistema (MS ActiveDirectory) galimybė, naudotojų autentifikavimui ir autorizavimui; - sistemos konteinerių saugumo ir stebėsenos įrankiai gali integruotis su saugumo stebėsenos įvykių valdymo (SIEM) įrankiais; - konteineriams yra uždrausta prisijungti prie pagrindinės (angl. „Host“) tarnybines stoties direktorijų. (pvz. System32, "etc", bin); - aplikacijų kopijų (angl. „images“) pažeidžiamumas yra tikrinamas kūrimo metu, o aplikacijų kopijos esančios registre tikrinamos kasdien; - sistema palaiko duomenų šifravimą (angl. encryption at rest);

		- sistema turi atitikti CIS Benchmark gerąsias konfigūravimo praktikas.	- sistema atitinka CIS Benchmark gerąsias konfigūravimo praktikas.
13.	Įrangos Suderinamumas	Siūlomos sistemos programinė įranga turi būti oficialiai palaikoma VMware programinės įrangos gamintojo.	Siūlomos sistemos programinė įranga oficialiai palaikoma VMware programinės įrangos gamintojo
14.	Programinės įrangos Palaikymas	Programinė įranga turi būti komplektuojama su 36 mėn. programinės įrangos gamintojo palaikymu ir versijų atnaujinimu. Techninis gedimų palaikymas teikiamas 24x7 sąlygomis, reaguojant į kritinį pranešimą apie gedimą ne vėliau kaip per 4 val. Pateikiamas gamintojo palaikymas turi užtikrinti teisę pirkėjui 3 m. laikotarpyje atsisiųsti gamintojo išleidžiamus programinės įrangos pataisymus, atnaujinimus ar naujausias versijas. Palaikymas turi būti teikiamas telefonu, elektroniniu paštu, nuotoliniu prisijungimu. Į kainą turi būti įskaičiuota programinės įrangos gamintojo konsultacijos licencijų naudojimo, diegimo ir palaikymo klausimais – ne mažiau nei 160 val.	Programinė įranga komplektuojama su 36 mėn. programinės įrangos gamintojo palaikymu ir versijų atnaujinimu. Techninis gedimų palaikymas teikiamas 24x7 sąlygomis, reaguojant į kritinį pranešimą apie gedimą ne vėliau kaip per 4 val. Pateikiamas gamintojo palaikymas užtikrina teisę pirkėjui 3 m. laikotarpyje atsisiųsti gamintojo išleidžiamus programinės įrangos pataisymus, atnaujinimus ar naujausias versijas. Palaikymas teikiamas telefonu, elektroniniu paštu, nuotoliniu prisijungimu. Į kainą įskaičiuota programinės įrangos gamintojo konsultacijos licencijų naudojimo, diegimo ir palaikymo klausimais – ne mažiau nei 160 val.
Reikalavimai programinės įrangos diegimui ir UŽSAKOVO informacinių išteklių galimybės konvertuoti į konteinerių technologijas analizės paslaugoms:			
15.	Reikalavimai sistemos diegimui ir dokumentacijai	Tiekėjas, per 20 kalendorinių dienų nuo UŽSAKOVO pranešimo gavimo dienos, turi pateikti sistemos diegimo projektinę dokumentaciją suderinta su Užsakovu. Dokumentacijoje reikės: - Įvertinti visas turimas aplikacijas/sistemas naudojant debesijai analizuoti tinkamą įrankį (pvz. „Cloud Suitability Analyzer“ arba lygiavertį); - Pateikti sąrašą sistemų, kurias rekomenduojama modernizuoti, remiantis šiuolaikinėmis geriausiomis pasaulio praktikomis; - Pateikti aplikacijų modernizavimo darbų rekomendacijas; - Pateikti modernizuojamų aplikacijų migravimo į	Tiekėjas, per 20 kalendorinių dienų nuo UŽSAKOVO pranešimo gavimo dienos, pateiks sistemos diegimo projektinę dokumentaciją suderintą su Užsakovu. Dokumentacijoje bus: - Įvertintas visas turimas aplikacijas/sistemas, naudojant debesijai analizuoti tinkamą įrankį (pvz. „Cloud Suitability Analyzer“ arba lygiavertį); - Pateiktas sąrašas sistemų, kurias rekomenduojama modernizuoti, remiantis šiuolaikinėmis geriausiomis pasaulio praktikomis; - Bus pateiktos aplikacijų modernizavimo darbų rekomendacijos; - Bus pateiktas modernizuojamų aplikacijų migravimo į produkcines aplinkas planas suderintas su Užsakovu;

		produkcines aplinkas planą, suderintą su Užsakovu; - Atlikus aplikacijų įvertinimą, Tiekėjas turi pateikti įžvalgų sąrašą, kuris būtų naudojamas modernizuojant aplikacijas ateityje; - Pateikti apžvalgą ir išvadas kurios turės apimti: - Turimų aplikacijų ir platformų įvertinimą; - Rekomendacijas programinei įrangai modernizuoti, turimų platformų galimybių sritis, numatytų darbų tikslus ir rizikų įvertinimą; - Platformų ir aplikacijų galimybių sričių identifikavimą; - Rezultatais pagrįstą planą kaip pasiekti pagrindinius veiklos tikslus, remiantis analizės išvadomis; - Didžiausių rizikų, hipotezių ir prielaidų sprendimo planą; - Saugumo, stabilumo ir funkcijų vystymo planą. - Pateikti planuojamo atlikti audito proceso aprašą; - Vadovautis 5S ir 5R metodologijomis; - Pateikti sistemos diegimo planą bei konfigūracijos aprašą; - Pateikti sistemos testavimo strategiją t.y. planą, scenarijus ir galimus rezultatu; - Pateikti paslaugų perėjimo bei atkūrimo planą; - Tiekėjas turės atlikti sistemos diegimą (sutartyje nustatytais terminais) pagal pateiktą projektinę dokumentaciją bei visus reikalingus parduodamos įrangos registravimo darbus gamintojo pagalbos tarnybos sistemoje.	- Atlikus aplikacijų įvertinimą, Tiekėjas pateiks įžvalgų sąrašą, kuris būtų naudojamas modernizuojant aplikacijas ateityje; - Pateiks apžvalgą ir išvadas kuriose bus: - Turimų aplikacijų ir platformų įvertinimas; - Rekomendacijas programinei įrangai modernizuoti, turimų platformų galimybių sritis, numatytų darbų tikslus ir rizikų įvertinimą; - Platformų ir aplikacijų galimybių sričių identifikavimą; - Rezultatais pagrįstą planą kaip pasiekti pagrindinius veiklos tikslus, remiantis analizės išvadomis; - Didžiausių rizikų, hipotezių ir prielaidų sprendimo planą; - Saugumo, stabilumo ir funkcijų vystymo planą. - Pateiks planuojamo atlikti audito proceso aprašą; - Vadovausis 5S ir 5R metodologijomis; - Pateiks sistemos diegimo planą bei konfigūracijos aprašą; - Pateiks sistemos testavimo strategiją t.y. planą, scenarijus ir galimus rezultatus; - Pateiks paslaugų perėjimo bei atkūrimo planą; - Tiekėjas atliks sistemos diegimą (sutartyje nustatytais terminais) pagal pateiktą projektinę dokumentaciją bei visus reikalingus parduodamos įrangos registravimo darbus gamintojo pagalbos tarnybos sistemoje.

Valdas Jusius

(vardas, pavardė)