ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS TECHNINĖ SPECIFIKACIJA

1. VšĮ Kauno miesto poliklinika perka antivirusinę programinę įrangą.

2. Kartu su pasiūlymu Tiekėjas turi pateikti **dokumentus, patvirtinančius siūlomos prekės atitikimą visiems reikalavimams, nurodytiems kiekviename pirkimo dokumentų techninės specifikacijos punkte, t. y. tiekėjas privalo pateikti siūlomų prekių gamintojo katalogus/ bukletus/ brošiūras, naudojimo instrukcijas su išsamiu siūlomų prekių techninių charakteristikų aprašymu** – prekės pavadinimu, modeliu (jei yra), gamintoju, kilmės šalimi, techninėmis charakteristikomis pagal techninės specifikacijos reikalavimus, prekių kodais (jei taikoma) bei visa informacija, pagrindžiančia **prekės atitikimą techninei specifikacijai originalo ir lietuvių kalba.** *Pateikiami dokumentai tiesiogiai suformuoti elektroninėmis priemonėmis arba skaitmeninės dokumentų kopijos originalo ir lietuvių kalba.*

3. prekei pagaminti ir (ar) tiekti sunaudojama mažiau gamtos išteklių, prekei pagaminti, tiekti ir (ar) naudoti sunaudojama mažiau elektros energijos ir (ar) naudojami atsinaujinantys, ekologiški energijos ištekliai; prekei pagaminti naudojama mažiau ar visai nenaudojama pavojingųjų cheminių medžiagų, neteršiama aplinka ir nekeliamas pavojus sveikatai (vadovaujantis Aplinkos apsaugos ktiterijų taikymo tvarkos aprašo 4.4.1. – 4.4.3. punktais). *Pateikiama tiekėjo deklaracija, arba gamintojo techniniai dokumentai, arba kiti lygiaverčiai įrodymai. Pateikiami dokumentai tiesiogiai suformuoti elektroninėmis priemonėmis arba skaitmeninės dokumentų kopijos originalo ir lietuvių kalba.*

Eil. nr.	**Gaminio techninė specifikacija**	**Atitikimas kokybiniams ir techniniams reikalavimams. Nuoroda į pridedamus, prekės atitikimą reikalaujamoms charakteristikoms įrodančius, dokumentus (bukletų, techninių aprašų puslapių Nr.)**		
		Siūlomos prekės pavadinimas, modelis, gamintojas, techniniai parametrai	**Pasiūlymo dokumentai, patvirtinantys siūlomos prekės techninius parametrus**	
			dokumento pavadinimas	**pasiūlymo lapo numeris**
1.	**Bendrieji reikalavaimai antivirusinei programinei įrangai**			
	Kliento – serverio principu veikianti integruota antivirusinė programinė įranga. Vartotojų kiekis – 90 vnt., laikotarpis - 24 mėnesiai.			
	Turi būti užtikrinta teisė gauti iš gamintojo naujausias programinės įrangos versijas.			
	Programinė įranga turi atitikti BDAR reikalavimus			
1.1	**Programinė įranga turi turėti šiuos funkcionalumus:** • Centrinio valdymo konsolė, veikianti debesyje • Fizinių kompiuterinių darbo vietų (stacionarieji ir nešiojami kompiuteriai) ir fizinių serverių (tarnybinės stotys) apsauga; • Virtualiųjų aplinkų apsauga; • Žinomų ir nežinomų trečiųjų šalių programinės įrangos spragų išnaudojimo apsauga; • Apsaugoti nuo tinklu plintančių atakų; • Apsaugoti nuo failus šifruojančių virusų atakų	• Centrinio valdymo konsolė, veikianti debesyje • Fizinių kompiuterinių darbo vietų (stacionarieji ir nešiojami kompiuteriai) ir fizinių serverių		

		(tarnybinės stotys) apsauga; • Virtualiųjų aplinkų apsauga; • Žinomų ir nežinomų trečiųjų šalių programinės įrangos spragų išnaudojimo apsauga; • Apsaugoti nuo tinklu plintančių atakų; Apsaugoti nuo failus šifruojančių virusų atakų		
1.2	**Bendri funkciniai reikalavimai antivirusinei programinei įrangai**			
	Turi būti galimybė nustatyti maksimalų skanuojamų failų dydį, kad būtų išvengta labai didelių failų skanavimo taip apkraunant sistemą.	Atitinka		
	Programinė įranga turi turėti atlikti išorinių laikmenų (CD, išoriniai kietieji diskai, atminties raktai) skenavimą.	Atitinka		
	Programinė įranga turi leisti išskirti pasirinktinai failus, aplankus, failų plėtinius, diskus ir procesus kurie būtų neskanuojami.	Atitinka		
	Programinė įranga turi saugoti nuo šnipinėjimo programų (angl. Spyware).	Atitinka		
	Programinė įranga turi sugebėti analizuoti HTTP ir HTTPs paketus.	Atitinka		
	Programinė įranga turi turėti apsaugos nuo fišingo funkcionalumą, kuris tikrintų interneto nuorodas ir blokuotų netinkamas.	Atitinka		
	Programinė įranga turi saugoti nuo išpirkos reikalaujančios ir sistemą užšifruojančios kenkėjiškos programinės įrangos (angl. Ransomware).	Atitinka		
	Programinė įranga turi apsaugoti nuo tinklu plintančių atakų, kurių metu yra bandoma neteisėtai gauti prieigą prie galutinio vartotojo įrenginio, suteikiant galimybę apsaugoti nuo grubios jėgos atakų (angl. Brute-force).	Atitinka		
	Programinė įranga turi apsaugoti nuo šifruojančių virusų atakų, o joms įvykus, sugebėti automatiškai atkurti palaikomus užšifruotus failus iš momentinės (laikinos) atsarginės kopijos be išorinių, papildomų techninių ar programinių resursų panaudojimo.	Atitinka		
	Galimybė centralizuotai patikrinti įrenginių operacinės sistemos ir tinklo nustatymų saugumą, naudojamos programinės įrangos pažeidžiamus ir rizikingą įrenginių naudotojų elgseną.	Atitinka		
1.3	**Reikalavimai klientų ugniasienei**			

	Klientų ugniasienė turi būti valdoma centralizuotai iš centrinės valdymo konsolės;	Atitinka		
	Klientų ugniasienė turi turėti galimybę padaryti kompiuterį/serverį nematomu tiek vietiniame tinkle, tiek ir internete. Šis nustatymas leidžia išjungti/blokuoti „ping“ ir kitas užklausas pasiekiančias kompiuterį/serverį.	Atitinka		
	Klientų ugniasienė gali būti įdiegta arba išdiegta konkrečiame įrenginyje pagal administratoriaus pasirinkimą.	Atitinka		
1.4	**Reikalavimai karantinui**			
	Turi būti galimybė automatiškai pašalinti į karantiną patekusius failus ir leisti administratoriui nustatyti, po kiek laiko, kai failai patenka į karantiną, tai bus atliekama.	Atitinka		
	Turi būti galimybė grąžinti failą iš karantino į ten kur jis buvo iki pakliūdamas į karantiną ar kitą vietą.	Atitinka		
	Turi būti galimybė atstatytiems failams automatiškai sukurti išimtis, kad jie pakartotinai nepakliūtų į karantiną.	Atitinka		
1.5	**Reikalavimai duomenų apsaugos funkcionalumui**			
1.6	**Reikalavimai vartotojų valdymui**			
	Programinė įranga turi turėti šį vartotojų kontrolės funkcionalumą: • Interneto prieigos blokavimas konkrečiam vartotojui ar vartotojų grupei. • Interneto blokavimas nustatytais laiko intervalais. • Prieigos blokavimas prie nustatytų aplikacijų. • Interneto puslapių prieigos blokavimas pagal raktažodžius. • Interneto puslapių prieigos blokavimas pagal kategorijas (netinkamo turinio puslapiai, azartinių žaidimų puslapiai ir pan.). • Leidimas pasiekti tik nustatytus interneto puslapius.	Atitinka		
1.7	**Reikalavimai išorinių prievadų kontrolei**			
	Šis modulis valdomas bei sudiegiamas/išdiegiamas iš tos pačios centrinės valdymo konsolės kuri valdo ir likusias funkcijas.	Atitinka		
	Išorinių prievadų kontrolės modulis turi leisti/drausti vartotojams prijungti šių tipų išorinius įrenginius: • CDROM įrenginius • Fotografuojančius įrenginius • Spausdintuvus • Tinklo adapterius • Išorinius diskus	Atitinka		
	Turi būti galimybė leisti/neleisti kiekvieno tipo išorinį įrenginį.	Atitinka		
	Turi būti galimybė nustatyti išimtis.	Atitinka		

2.	**Reikalavimai centrinei valdymo konsolei**			
2.1	**Diegimas ir konfigūravimas**			
	Turi būti galimybė be papildomų mokesčių ar saugomų įrenginių skaičiaus apribojimų, programinių ar aparatūrinių priemonių debesyje paleisti ir naudoti centrinę valdymo konsolę.	Atitinka		
2.2	**Bendri reikalavimai centrinei valdymo konsolei**			
	Turi turėti automatinę pranešimų sistemą, kuri informuotu apie: • antivirusinės programinės įrangos licencijos panaudojimo perviršį; • antivirusinės programinė įrangos atnaujinimus; • aptinkamą kenksmingą programinę įrangą ir jos nukenksminimą.	Atitinka		
	Pranešimai apie įvykius atvaizduojami konsolėje bei siunčiami nurodytu elektroniniu paštu.	Atitinka		
	Turi būti galimybė reguliuoti pranešimų jautrumą – lygį nuo kurio generuojamas aliarmas (pavyzdžiui laiko tarpas, kurį viršijus kompiuterio antivirusinė programa traktuojama kaip pasenusi (angl. Outdated)	Atitinka		
	Ataskaitos turi būti generuojamos pagal numatytą grafiką arba rankiniu būdu ir pateikiamos grafiniame formate.	Atitinka		
	Turi būti galimybė nustatyti kokias konkrečias ataskaitas gaus kiekvienas iš antivirusinės programinės įrangos administratorių.	Atitinka		
2.3	**Inventorizavimas ir valdymas**	Atitinka		
	Programinė įranga gali būti integruojama su Active Directory domenais..			
	Turi būti galimybė nustatyti ir derinti saugumo politikas pagal: • Fizinį įrenginį; • Lokaciją; • Vartotoją	Atitinka		
	Su klientine programine įranga ar be jos fizinių ir virtualių įrenginių paieška ir rūšiavimas pagal kompiuterio vardą, operacinę sistemą, naudotojo vardą ir IP adresą.	Atitinka		
	Nuotolinis klientinio modulio diegimas, sudarant galimybę pasirinkti, ar prieš tai išinstaliuoti buvusią antivirusinę programinę įrangą (t. y. galimybė veikti prieš tai buvusiai ir naujai įdiegtai antivirusinėms programinėms įrangoms).	Atitinka		
2.4	**Funkciniai reikalavimai programinės įrangos administratorių valdymui**			
	Programinė įranga turi leisti nustatyti roles skirtingoms administravimo teisėms. Programinės įrangos administratoriai gali būti importuojami iš Active Directory domeno ir sinchronizuojamas autentifikavimas (angl. Single Sign On).	Atitinka		
2.5	**Reikalavimai registrui (angl. Logs)**			

	Turi būti fiksuojami ir išsaugomi visi centrinės valdymo konsolės administratorių veiksmai.	Atitinka		
	Centrinė valdymo konsolė saugo registrų įrašų su informacija apie administratorių atliktus veiksmus: kada prisijungta, kas koreguota, sukurta, atsijungta, perkelta ir panašiai,	Atitinka		
	Programinė įranga turi turėti registro įrašų paiešką pagal administratorių veiksmus ir laiko intervalą.	Atitinka		
2.6	**Reikalavimai sertifikatų valdymui**			
	Prie programinės įrangos valdymo jungiamasi naudojant HTTPs protokolą.	Atitinka		
	Saugumo užtikrinimui naudojami skaitmeniniai sertifikatai.	Atitinka		
	Turi būti galimybė centrinėje valdymo konsolėje peržiūrėti sertifikatų informaciją (išdavusios organizacijos pavadinimas, išdavimo ir galiojimo datos).	Atitinka		
3.	**Reikalavimai kompiuterinių darbo vietų (stacionarieji ir nešiojamieji kompiuteriai) ir serverių (tarnybinės stotys) apsaugos moduliui**			
3.1	**Bendri reikalavimai**			
	Kompiuterinių darbo vietų (stacionarieji ir nešiojami kompiuteriai) modulis privalo turėti bent šiuos funkcionalumus: • apsauga nuo kenkėjiškos programinės įrangos; • turinio kontrolė; • išorinių įrenginių kontrolės; • ugniasienė.	Atitinka		
3.2	**Patyrusio vartotojo funkcionalumas (angl. Power User)**			
	Modulis gali būti įdiegtas ar išdiegtas administratoriaus iš centrinės valdymo konsolės.	Atitinka		
	Naudojant patyrusio vartotojo modulį vartotojas panaudojęs slaptažodį gauna prieiga prie programinės įrangos klientinės dalies nustatymų.	Atitinka		
3.3	**Reikalavimai modulio diegimui ir valdymui**			
	Prieš diegimą centrinės valdymo konsolės pagalba administratorius gali sukomplektuoti instaliacinį failą su reikiamais moduliais (ugniasienės, turinio kontrolės, išorinių įrenginių kontrolė)	Atitinka		
	Turi būti galimi šie modulio diegimo būdai: • Parsisiunčiant instaliacinį failą tiesiai į kompiuterį; • Diegiant iš centrinės valdymo konsolės.	Atitinka		
	Centrinėje valdymo konsolėje galime peržiūrėti detalią informaciją apie kiekvieną kompiuterį ir serverį: kompiuterio/serverio vardas, IP adresas, operacinė sistema, įdiegti antivirusinės programos elementai, nustatyta politika, virusų aprašų versija.	Atitinka		

	Palaikomos operacinės sistemos: ● Windows 10 ● Windows 8.1 ● macOS Monterey (12.x) ● macOS Big Sur (11.x)	Atitinka		

Dokumentą elektroniniu parašu pasirašė EVALDAS,URBONAS
Data: 2022-05-03 13:38:16