2022 m. d.
prekių viešojo
pirkimo-pardavimo sutarties
1 priedas

ANTIVIRUSINĖS PROGRAMINĖS ĮRANGOS LICENCIJŲ TECHNINĖ SPECIFIKACIJA

1. Lietuvos Respublikos vidaus reikalų ministro valdymo sričiai priklausančiose įstaigose, kurių sąrašas pateiktas techninės specifikacijos priede (toliau – įstaigose prie VRM), naudojamas *„Sophos“* antivirusinės programinės įrangos licencijų paketas, susidedantis iš *antivirusinės programos „Sophos Intercept X Advanced“ licencijų naudotojui* ir *mobilių įrenginių valdymo programinės įrangos „Sophos Mobile Advanced“ licencijų naudotojui*. „Sophos“ antivirusinės programinės įrangos licencijos užtikrina įstaigose prie VRM esančių kompiuterizuotų darbo vietų ir mobilių darbo vietų apsaugą nuo visų rūšių virusų, šnipinėjimo ir kenksmingų programų, išorinių įsibrovimų ir programišių atakų bei elektroninio pašto šiukšlių.

2. Informatikos ir ryšių departamente prie Lietuvos Respublikos vidaus reikalų ministerijos įdiegta „Sophos“ centrinio valdymo konsolė, užtikrinanti centralizuotą antivirusinės programinės įrangos ir mobilių kompiuterizuotų darbo vietų valdymą bei apsaugą nuo rinkmenas užkoduojančios žalingos programinės įrangos (angl. *ransomware*).

3. Pirkimo tikslas – įsigyti papildomas „Sophos“ antivirusinės programinės įrangos licencijas „Sophos Intercept X Advanced“ įrenginiui, „Sophos Intercept X Advanced“ serveriui ir „Sophos Mobile Advanced“ licencijas naudotojui. Visos licencijos **turi galioti iki 2024 m. gruodžio 31 d.** Jeigu sutarties galiojimo laikotarpiu tiekėjas atnaujins antivirusinės programos paketo ir mobilių įrenginių valdymo, centrinės valdymo konsolės programinės įrangos versijas, palaikymas turi būti užtikrintas atnaujintoms programinės įrangos versijoms.

4. Pirkimo objektui taikomi Lietuvos Respublikos viešųjų pirkimų įstatymo 37 str. 9 dalies reikalavimai *susiję su nacionaliniu saugumu*.

5. Tiekėjas privalo įrodyti, kad prekės nekelia grėsmės nacionaliniam saugumui, nėra toliau nurodytų aplinkybių:

5.1. prekių gamintojas ar jį kontroliuojantis asmuo yra registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) VPĮ 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose;

5.2. prekių priežiūra ar palaikymas būtų vykdomas iš VPĮ 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų.

6. Tiekėjas turi būti programinės įrangos gamintojas arba gamintojo įgaliotas atstovas, turintis teisę tiekti, diegti bei aptarnauti programinę įrangą (jei tiekėjas pats nėra gamintojas). Pateikiamos tai patvirtinančių dokumentų kopijos.

7. Tiekėjas Sutarties vykdymui turi turėti internetu pasiekiamą ir visą parą veikiančią IT pagalbos tarnybos informacinę sistemą arba įvykių registracijos sistemą, leidžiančią registruoti įrangos sutrikimus, sužinoti atliktų darbų šalinant sutrikimus eigą ir esamąją sutrikimo šalinimo būseną. Pateikiamas dokumentas, kuriame turi būti nurodyta: telefono numeris, IT pagalbos informacinės sistemos arba įvykių registracijos sistemos el. pašto adresas, IT pagalbos informacinės sistemos arba įvykių registracijos sistemos adresas internete.

8. Tiekėjas turi užtikrinti, kad Sutartį visą Sutarties galiojimo laikotarpį vykdys pasiūlyme nurodyti ir Sutarties reikalavimus atitinkantys specialistai. Sutarties galiojimo metu nurodyti specialistai gali būti pakeisti kitais (specialistui susirgus, patyrus traumą, pakeitus darbovietę, atsisakius vykdyti funkcijas) tik gavus rašytinį Kliento sutikimą. Keičiami specialistai turi atitikti

pirkimo sąlygose nurodytus reikalavimus: Tiekėjas Sutarties vykdymui privalo turėti antivirusinės programinės įrangos diegimo specialistą (ne mažiau kaip 1 (vienas) specialistas), kuris turi atitikti žemiau nurodytus reikalavimus:

8.1. turi turėti antivirusinės programinės įrangos specialisto diegimo ir/ar palaikymo kvalifikaciją, patvirtintą antivirusinės programinės įrangos gamintojo išduotu sertifikatu arba lygiaverčio dokumentu;

9. Minimalūs „Sophos“ antivirusinės programinės įrangos licencijų techniniai reikalavimai pateikti lentelėje:

Eil. Nr.	**Pavadinimas, parametras**	**Minimalūs reikalavimai**
1.	Antivirusinės programinės įrangos paskirtis	Centralizuotai apsaugoti kompiuterizuotas darbo vietas (KDV) ir serverius nuo visų rūšių virusų, šnipinėjimo ir kenksmingų programų (*spyware*), išorinių įsibrovimų ir programišių atakų. Užtikrinti mobilių KDV valdymą, apsaugoti nuo rinkmenas užkoduojančių žalingos programinės įrangos (angl. *ransomware*). Turi būti valdoma iš „Sophos“ centrinio valdymo konsolės.
2.	Gamintojas, pavadinimas	Turi būti nurodytas antivirusinės programos pavadinimas ir tiksli nuoroda į gamintojo interneto puslapį, kuriame pateikta visa informacija apie siūlomą prekę.
3.	Antivirusinės programinės įrangos diegimas	Turi būti centrinio valdymo konsolė, užtikrinanti centralizuotą antivirusinės programinės įrangos ir mobilių KDV valdymą, turi būti sukonfigūruota siūlomo gamintojo debesijos aplinkoje. Programinės įrangos konfigūravimą turi užtikrinti specialistas, kurio kvalifikacija turi būti patvirtinta siūlomos programinės įrangos gamintojo išduotu sertifikatu arba lygiaverčiu dokumentu.
4.	Bendrieji reikalavimai	Turi turėti tokias integruotas funkcijas: • antivirusinę sistemą apsaugai nuo žalingų programų; • kategorijomis paremtą naršymo kontrolę; • išorinių kompiuterizuotos darbo vietos sąsajų kontrolę; • kompiuterizuotai darbo vietai skirtos ugniasienės valdymą; • aplikacijų kontrolės funkcionalumą; • mobilių įrenginių valdymo funkcionalumą; • apsaugos nuo interneto grėsmių ir filtravimo funkcionalumą; • apsaugą nuo programinės įrangos klaidos išnaudojimo (angl. *exploit prevention*); • apsaugą nuo failus užkoduojančių virusų (angl. *ransomware prevention*; • duomenų nutekėjimo prevencijos kompiuterizuotoje darbo vietoje funkcionalumą; • priežasties-pasekmės analizės įrankį (angl. *root cause analysis tool*); • centralizuotą saugumo komponentų valdymo konsolę, veikiančią debesijos pagrindu.

		Nurodyto funkcionalumo užtikrinimui gali būti pateikti keli atskiri vieno gamintojo produktai, turintys vieną bendrą visiems produktams ar kelis atskirus centralizuoto valdymo įrankius.
		Centralizuoto valdymo įrankis turi valdyti ne mažiau kaip šiuos siūlomos programinės įrangos komponentus: • antivirusinę sistemą; • naršymo internete kontrolę; • apsaugos nuo rinkmenas užkoduojančių virusų funkcionalumą; • išorinių kompiuterizuotos darbo vietos sąsajų kontrolę; • kompiuterizuotai darbo vietai skirta ugniasienę; • aplikacijų kontrolės funkcionalumą; • apsaugos nuo interneto grėsmių ir filtravimo funkcionalumą; • duomenų nutekėjimo prevencijos kompiuterizuotoje darbo vietoje funkcionalumą.
		Turi palaikyti virtualias KDV ir tarnybines stotis šiose platformose (neturi reikalauti atskiros licencijos virtualios infrastruktūros apsaugai): • *VMware vSphere / ESX;* • *VMware Workstation;* • *VMware View;* • *Citrix XenServer;* • *Citrix XenApp;* • *Microsoft Hyper-V Server.*
		KDV skirtas sprendimas turi apsaugoti ne mažiau kaip 2000 naudotojų. Naudotojui skirta licencija turi apsaugoti daugiau nei vieną kompiuterinį įrenginį t. y. programinė įranga turi būti licencijuojama ne per įrenginį ir viena licencija turėtų tikti apsaugai kelių įrenginių. Programinė įranga turi būti licencijuojama ne per įrenginį ir viena licencija turėtų tikti apsaugai iki 5 vieno naudotojo įrenginių. Pateikiamos licencijos turi apimti visą šioje specifikacijoje aprašytą funkcionalumą.
5.	Antivirusinės programos funkcionalumas	Turi užtikrinti apsaugą nuo virusų, *spyware, adware, ransomware* tipo žalingų programų, *rootkits*, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų.
		Sistema turi naudoti genotipo technologiją, kuri gebėtų proaktyviai blokuoti virusus prieš pasirodant virusų aprašų duomenų bazėms.
		Turi atlikti žalingų veiksmų stebėseną ir aptikti dar nežinomą žalingą programinę įrangą, tiek prieš paleidžiant/atidarant rinkmeną, tiek skaitant, įrašant ar pervadinant failą, tiek po rinkmenos paleidimo turi būti analizuojamas jos elgesys.
		Sistema turi gebėti sustabdyti ne mažiau kaip 20 exploit technikų įskaitant: • APC naudojimo (*Application Procedure Calls*); • Privilegijų eskalavimo ataka (*privilege escalation*).

Sistema turi gebėti sustabdyti šifravimo atakas: • Failų kodavimo apsauga (*ransomware*); • Master Boot Record kodavimo apsauga.
Sistema turi gebėti išanalizuoti paleidžiamojo failo parametrus bei naudojamas funkcijas naudojant neuro-tinklus ir pagal juos prognozuoti kiek labai tas failas pavojingas, taip pat turi gebėti palyginti failą su jau žinomais pavojingais ar žinomais gerais failais. Tuomet pagal visą surinktą informaciją nuspręsti ar vykdyti failą.
Turi aptikti kenkėjišką internetinį srautą (angl. *malicious traffic*) į komandų ir kontrolės centrus (angl. *command and control center*) ir jį blokuoti.
Turi tikrinti kenkėjišką kodą paleidžiamuosiuose failuose, taip pat dokumentuose turinčiuose aktyvių elementų, tokių kaip makros komandos ir skriptai.
Turi aptikti kenkėjišką kompiuterio programų elgesį naudojant sisteminių atakų prevencijos sistemą (angl. *HIPS*).
Turi atsinaujinti ne mažiau kaip du kartus per dieną.
Turi užtikrinti skenavimą prieigos prie rinkmenų metu ir sistemos krovimosi metu.
Turi leisti nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus ir turi būti galimybė skirti nurodyta kompiuterio resursų kiekį šiam skenavimui.
Turi galėti automatiškai atlikti išvalymą nuo aptiktų žalingų programų.
Turi apsaugoti internetines naršykles (tokias kaip *Internet Explorer, Edge, Firefox, Chrome, Safari, Opera*), blokuojant prieigą prie žinomų kenksmingų tinklalapių ir skenuojant atsiunčiamus duomenis prieš jų paleidimą/atidarymą.
Turi leisti numatyti išimtis specifinių direktorijų ar rinkmenų skenavimui.
Turi galėti skenuoti ne mažiau kaip šiais standartais archyvuotas rinkmenas: 7z, zip, arj, bzip2, gzip, MS cab, rar, tar.
Turi gebėti atpažinti failo tipą, t. y. atlikti failo tipo nustatymą ne tik pagal failo tipo plėtinį.
Turi užtikrinti saugumą nešiojamiems ir staliniams kompiuteriams, tarnybinėms stotims, mobiliems įrenginiams.
Turi galėti aptikti polimorfines virusų atmainas.

		Turi galėti blokuoti įtartinas rinkmenas mažiausiai pagal tokius kriterijus: • Naudojamas dvigubas plėtinys; • Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pav. exe tipo rinkmena yra įvardijama, kaip .txt).
		Turi galėti atlikti *JavaScript* emuliaciją ir elgesio analizę, siekiant užtikrinti apsaugą nuo internetu platinamo žalingo kodo.
		Turi užtikrinti „keliaujančių“ kompiuterių saugų darbą internete, t. y. kai kompiuteris yra ne organizacijos tinkle. Turi gebėti patikrinti interneto svetainės turinį, prieš jį pateikiant naudotojo internetinei naršyklei, pagal tokius parametrus: • Įvertinti, ar lankoma svetainė nepatenka į infekuotų ir pavojingų tinklalapių sąrašą; • Taikyti svetainių filtravimą pagal kategorijas.
		Turi būti negalima išjungti sistemos nustatymų eiliniam naudotojui, įskaitant naudotojus, turinčius lokalaus administratoriaus teises kompiuteryje.
		Turi palaikyti ir apsaugoti 32/64 bit *Windows, bei 64 bit macOS* operacines sistemas.
		Turi turėti integruotą karantino paskyrą. Administratorius turi galėti leisti prieigą pasirinktiems naudotojams prie jų karantino paskyros, kur naudotojai minimaliai galėtų atlikti šiuos veiksmus: • Išvalyti užkrėstą rinkmeną; • Perkelti užkrėstą rinkmeną; • Ištrinti užkrėstą rinkmeną.
		Siūlomas produktas informacinių technologijų tyrimo įstaigos *Gartner* (http://www.gartner.com) 2021 metų duomenimis turi būti tarp lyderiaujančių produktų (*Leaders* kategorijoje) darbo vietų apsaugos platformų grupėje (*Magic Quadrant for Endpoint Protection Platforms*).
6.	Apsaugos nuo failus užkoduojančių virusų (angl. *ransomware prevention*) funkcionalumas	Siūlomas sprendimas turi turėti funkcionalumą skirtą apsaugai nuo failus užkoduojančių virusų ir turi būti valdomas iš centralizuotos valdymo konsolės.
		Turi blokuoti failus užkoduojančius virusus be virusų aprašų duomenų bazių (angl. *signatureless prevention*);
		Turi stebėti visus vykstančius šifravimo procesus ir blokuoti tik tuos šifravimo procesus, kurie yra inicijuoti failus užkoduojančių virusų, t.y. iš neautorizuotų procesų.
		Jeigu sprendimas aptinka žalingą šifravimo procesą leisdamas užšifruoti tam tikrą kiekį failų, sprendimas prieš tai turi sukurti tų failų kopijas ir patalpinti laikiname podėlyje. Jeigu neautorizuotas procesas buvo užblokuotas, užšifruoti failai turi būti automatiškai atkuriami.

7.	Sistemos centralizuotas valdymas, administravimas ir konfigūravimas	Siūlomo sprendimo centralizuoto valdymo konsolė turi valdyti apsaugos sistemas šiose platformose: *Windows ir Mac.*
		Siūlomo sprendimo atnaujinimas KDV turi vykti tiesiai iš gamintojo atnaujinimo serverio internetu, o taip pat turi būti galimybė automatiškai parsisiųsti atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete.
		Turi būti galimybė numatyti pirminį ir antrinį atnaujinimo serverius. Jei KDV yra lokaliame tinkle, tai KDV siunčiasi atnaujinimus iš lokalaus atnaujinimų serverio (pirminis serveris). Jei ta pati KDV naudojama už organizacijos tinklo perimetro ribų, tai atnaujinimus turi galėti parsisiųsti iš gamintojo serverio internetu arba iš serverio patalpinto organizacijos DMZ zonoje (antrinis serveris).
		Siūlomas sprendimas turi leisti nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus, sistema išsiųstų el. paštu įspėjimą.
		Siūlomas sprendimas turi leisti grupuoti, filtruoti ir rūšiuoti apsaugotus kompiuterius centralizuoto valdymo konsolėje minimaliai pagal šiuos parametrus: • *Active Directory Organization Unit*; • OS tipą/versiją; • Pagal IP adresą; • Pagal atnaujinimo būklę; • Pagal kompiuterio būklę.
		Turi būti galimybė sistemos administratoriui nuotoliniu būdu išspręsti problemas, pasirenkant vieną ar keletą kompiuterių, „vienu mygtuko paspaudimu“ šiems veiksmams: • Apsaugoti kompiuterį, įdiegiant ar pakartotinai įdiegiant apsaugos programinę įrangą; • Priverstinai paleisti atnaujinimą; • Paleisti pilną sistemos skenavimą; • Pašalinti įspėjamuosius pranešimus; • Priverstinai pritaikyti nustatytąją saugumo politiką; • Perkelti pasirinktus kompiuterius į kitą grupę (taisyklės turi būti taikomos automatiškai pagal naują grupę); • Ištrinti kompiuterį iš sąrašo.
		Siūlomo sprendimo centralizuoto valdymo konsolė turi integruotis su Microsoft Active Directory ir veiksmai atliekami direktorijoje turi būti sinchronizuojami su saugumo sprendimo centralizuoto valdymo konsole. Pašalinus naudotoją ar grupę iš Active Directory, tie patys įrašai automatiškai turi būti pašalinami ir iš saugumo sprendimo centralizuoto valdymo konsolės.
		Siūlomas sprendimas turi leisti taikyti nustatytąją saugumo politiką grupei valdomų kompiuterių arba individualiems kompiuteriams;
		Siūlomas sprendimas turi leisti rolėmis su skirtingomis administravimo teisėmis paremtą administravimą;

		Siūlomas sprendimas turi galėti registruoti administratoriaus veiksmus auditavimo tikslais;
		Siūlomas sprendimas turi turėti integruotą ataskaitų įrankį, kuris ataskaitų generavimui naudotų visą informaciją esančią saugumo sistemos duomenų bazėje. Ataskaitos turi būti generuojamos pagal numatytą grafiką arba rankiniu būdu ir pateikiamos grafiniame formate. Ataskaitas turi būti galima automatiškai išsiųsti el.paštu minimaliai šiais formatais: pdf, csv;
8.	Išorinių KDV sąsajų ir aplikacijų kontrolė	Siūlomas sprendimas turi leisti nustatyti, kuriems kompiuteriams leidžiama prieiga nustatytiems išoriniams įrenginiams.
		Siūlomas sprendimas turi galėti kontroliuoti ne mažiau kaip šio tipo išorinius įrenginius: • išorinės atminties talpos įrenginius (įrenginiai pajungiami per USB2/3 prievadus); • CD ir DVD įrenginius; • Floppy įrenginius; • Infraraudonąją jungtimi prijungiamus įrenginius; • *Wifi* įrenginius; • *Bluetooth* jungtimi prijungiamus įrenginius.
		Siūlomas sprendimas turi leisti priskirti išorinio įrenginio naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms.
		Siūlomas sprendimas turi leisti atlikti sekančius veiksmus įrenginiams: • Leisti prijungti visus to paties modelio įrenginius; • Leisti naudoti įrenginį pagal jo unikalų identifikacijos numerį; • Leisti įrenginiui prisijungti pilnomis teisėmis; • Leisti įrenginiui prisijungti tik „skaitymo“ režime.
		Siūlomas sprendimas turi turėti galimybę blokuoti „*bridge“* režimą tarp laidinio ir bevielio tinklo tame pačiame įrenginyje neprarandant interneto prieigos.
		Siūlomo sprendimo įrenginių kontrolei pasiekti turi būti valdomas iš tos pačios naudotojo aplinkos (*UI*), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.
		Sistema turi leisti kontroliuoti programas (ang. *applications*), siekiant užtikrinti tinklo resursų išnaudojimą ir saugumą. Sąrašas kontroliuojamų aplikacijų turi apimti, neapsiribojant, tokias aplikacijas, kaip rinkmenų keitimosi programos (pav. *torrent, p2p*), greitųjų žinučių apsikeitimo programos (pav. *Skype*), žaidimai ir t.t.
		Sistema turi užtikrinti automatinę kontroliuojamų programų naujų versijų atnaujinimo kontrolę, automatinį programų aptikimą ir blokavimą.
		Turi būti galimybė aplikacijas skirstyti į kategorijas (ne mažiau kaip 40 kategorijų).

		Siūlomas sprendimas turi galėti priskirti aplikacijų naudojimo politiką individualiems kompiuteriams ar kompiuterių grupėms.
1.8.	Duomenų nutekėjimo prevencijos (angl. *Data loss prevention*) funkcionalumas	Siūloma sistema turi turėti integruotą funkcionalumą duomenų iš kompiuterinės darbo vietos tyčinio ar netyčinio praradimo apsaugai.
		Sistema turi leisti nustatyti dokumentui žymą (požymį), pagal kurią vėliau būtų atliekama dokumento kontrolė (pav. neleisti dokumento su tam tikra žyma siųsti el. paštu, įkelti per naršyklę išsiuntimui į internetą, kopijuoti į nešifruotą išorinės talpos įrenginį ar persiųsti greitųjų žinučių apsikeitimo programa ir pan.)
		Siūlomos sistemos duomenų kontrolės funkcionalumas turi būti valdomas iš tos pačios naudotojo aplinkos (*UI*), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės.
		Siūloma sistema turi turėti gamintojo integruotą ir gamintojo atnaujinimą jautrios informacijos duomenų aprašų bazę.
		Siūloma sistema turi leisti pačiai organizacijai nustatyti turinį kontrolei ir taisykles, pasinaudojant nustatymo vedliu.
		Siūloma sistema turi registruoti veiksmus su kontroliuojamomis rinkmenomis.
		Sistema turi leisti nustatyti teisę naudotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai turi būti registruojami.
		Siūloma sistema turi atlikti duomenų kontrolę ne mažiau kaip per šiuos komunikacijos kanalus: • Siunčiant duomenis kaip priedėlį per el. pašto klientą; • Siunčiant/įkeliant duomenis per internetinę naršyklę; • Siunčiant duomenis per greitųjų žinučių apsikeitimo programas.
		Siūloma sistema turi turėti jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė.

Techninės specifikacijos priedas

Įstaigų sąrašas

1. Asmens dokumentų išrašymo centras prie Lietuvos Respublikos vidaus reikalų ministerijos.
2. Finansinių nusikaltimų tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos.
3. Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos.
4. Lietuvos Respublikos vidaus reikalų ministerijos Medicinos centras.
5. Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos.
6. Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos.
7. Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos.
8. Viešojo saugumo tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos.

PIRKĖJAS	**PARDAVĖJAS**
Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos	**Blue Bridge MSP, UAB**