SUTARTIS Nr. APVA/2021/08/10

UAB „NBCS“ (toliau – Vykdytojas), atstovaujama generalinio direktoriaus Artiom Maslov, veikiančio pagal įmonės įstatus, iš vienos pusės,
ir
Lietuvos Respublikos aplinkos ministerijos Aplinkos projektų valdymo agentūra (toliau – Užsakovas), atstovaujama Nacionalinių programų valdymo departamento direktoriaus, vykdančio direktoriaus funkcijas Jono Balkevičiaus, veikiančio pagal įstaigos nuostatus, iš kitos pusės, sudarėme ir pasirašėme šią Sutartį, kuria susitariame:

1. SUTARTIES DALYKAS

1.1. Vykdytojas įsipareigoja pagal techninėje specifikacijoje (Sutarties priedas Techninė specifikacija) pateiktas technines charakteristikas Užsakovui pateikti (pratęsti jau turimų licencijų galiojimą) Kompiuterinių darbo vietų bei tarnybinių stočių antivirusinės apsaugos ir kontrolės programinės įrangos licencijas (toliau – Licencijos), o Užsakovas įsipareigoja sumokėti už Licencijas šioje Sutartyje nustatyta tvarka.

2. PRISTATYMO TVARKA IR TERMINAI

2.1. Licencijų pratęsimo terminas įsigalioja nuo 2021 m. rugsėjo 17 d. Vykdytojas apie užsakytų licencijų įjungimą informuoja el. paštu itskyrius@apva.lt.

3. ATSISKAITYMŲ TVARKA

3.1. Užsakovas už Licencijas sumoka Vykdytojui tokiomis kainomis:

Eil. Nr.	**Pirkimo objektas**	**Licencijos pavadinimas**	**Mato vienetas**	**Kiekis**	**Kaina, EUR be PVM**
	1	*2*	*3*	*4*	*5*
1.	Kompiuterinių darbo vietų antivirusinės apsaugos ir kontrolės programinės įrangos licencijos 24 mėn. laikotarpiui	Central Intercept X Endpoint Advanced	vnt.	130	7020,00
2.	Tarnybinių stočių antivirusinės apsaugos ir kontrolės programinės įrangos licencijos 24 mėn. laikotarpiui	Central Intercept X Advanced for Server	vnt.	5	890,00
				Bendra kaina, Eur be PVM:	7910,00
				PVM suma, Eur:	1661,10
				Bendra kaina, Eur su PVM:	9571,10

3.2. Į Licencijų kainą privalo būti įskaičiuotos visos su Licencijų pristatymu susijusios išlaidos.
3.3. Vykdytojas už Licencijas įsipareigoja pateikti PVM sąskaitą faktūrą, kurią Užsakovas apmoka per 30 (trisdešimt) kalendorinių dienų nuo jos gavimo dienos. PVM sąskaitos faktūros privalo būti teikiamos naudojantis “E.sąskaita” sistema www.esaskaita.eu.

4. ŠALIŲ TEISĖS IR ĮSIPAREIGOJIMAI

4.1. Vykdytojas įsipareigoja:
4.1.1. pristatyti Licencijas šioje Sutartyje nustatytomis sąlygomis ir tvarka.
4.2. Vykdytojas turi teisę:
4.2.1. reikalauti, kad Užsakovas už pateiktas Licencijas sumokėtų pagal šios Sutarties 3.1. punkte nustatytas kainas.
4.3. Užsakovas įsipareigoja:
4.3.1. nupirkti Licencijas;
4.3.2. sumokėti už jas nustatytą kainą Sutartyje numatytomis sąlygomis ir tvarka.
4.4. Užsakovas turi teisę:
4.4.1. reikalauti pristatyti Licencijas;
4.4.2. pareikalauti atlyginti nuostolius, jeigu Vykdytojas, pažeisdamas Sutartį, nepateikia Licencijų Užsakovui Sutartyje numatytais terminais ir tvarka.
4.5. Jei Vykdytojas Sutartyje nustatytais terminais nepateikia Licencijų, tai jis sumoka delspinigius, kurie lygūs 0,02 % (dvi šimtosios procento) nuo nepristatytų Licencijų kainos už kiekvieną pradelstą dieną.
4.6. Jei Užsakovas per šios Sutarties 3.3. punkte nurodytą terminą neatsiskaito su Vykdytoju, jis privalo Vykdytojui sumokėti 0,02 % (dvi šimtosios procento) dydžio delspinigius nuo neapmokėtos sumos už kiekvieną uždelstą dieną.
4.7. Jei Vykdytojas su Užsakovu suderintais terminais nepateikia Licencijų ir vėluoja daugiau kaip 14 dienų, tai jis sumoka Užsakovui baudą, kurios dydis apskaičiuojamas sumažinant Licencijų įkainį 30 proc. ir atitinkamą sumą išskaičiuojant iš Užsakovui apmokėjimui pateiktos PVM sąskaitos faktūros. Baudos išskaičiavimas neatleidžia Vykdytojo nuo prievolės įvykdymo.
4.8. Vykdytojas įsipareigoja padengti visas išlaidas, susijusias su skolų išieškojimu, kurios susidarė dėl Vykdytojo kaltės.

5. KOKYBĖ

5.1. Licencijų kokybė turi atitikti gamintojo numatytus reikalavimus ir norminių dokumentų (standartų, techninių sąlygų, etalonų, pavyzdžių ir kt.) reikalavimus.

6. FORCE MAJEURE

6.1. Sutarties šalis atleidžiama nuo atsakomybės už savo įsipareigojimų nevykdymą, jeigu ji įrodo, kad šių įsipareigojimų nebuvo galima įvykdyti dėl nenugalimos jėgos (force majeure), kurios sutarties sudarymo momentu ši šalis negalėjo numatyti ir kurios ji negalėjo išvengti ar nugalėti.
6.2. Nustatant force majeure aplinkybes, taikomos Lietuvos Respublikos Vyriausybės 1996 07 15 nutarimo Nr. 840 nuostatos.

7. SUTARTIES GALIOJIMAS

7.1. Sutartis įsigalioja nuo priėmimo-perdavimo akto pasirašymo dienos ir galioja 24 (dvidešimt keturis) mėnesius.
7.2. Sutartis gali būti nutraukta raštišku abiejų šalių susitarimu arba vienos šalies iniciatyva Sutartyje ar Lietuvos Respublikos teisės aktuose numatytais pagrindais.
7.3. Kiekviena šalis gali vienašališkai nutraukti šią Sutartį prieš tai raštu pranešusi kitai Šaliai ne mažiau kaip 14 (keturiolika) kalendorinių dienų.

8. TAIKYTINA TEISĖ IR GINČŲ SPRENDIMAS

8.1. Sutarčiai taikoma Lietuvos Respublikos teisė.
8.2. Esant prieštaravimų tarp sutarties sąlygų ir Lietuvos Respublikos teisės aktų nuostatų, taikomos Lietuvos Respublikos norminių teisės aktų nuostatos.
8.3. Visi ginčai, kilę iš sutarties, sprendžiami derybų būdu. Nepavykus ginčų išspręsti derybų būdu, ginčai sprendžiami Lietuvos Respublikos įstatymų nustatyta tvarka.

9. SUTARTIES PRIEDAI IR KEITIMAS

9.1. Sutarties sąlygos sutarties galiojimo laikotarpiu negali būti keičiamos, išskyrus tokias sutarties sąlygas, kurias pakeitus nebūtų pažeisti Viešųjų pirkimų įstatymo nustatyti pagrindiniai principai ir tikslai.
9.2. Visi sutarties priedai laikomi neatskiriama jos dalimi:
9.2.1. viešojo pirkimo dalyvio UAB „NBCS“ laimėjęs pasiūlymas, 1 lapas (Sutarties priedas Nr. 1);
9.2.2. techninė specifikacija (Sutarties priedas Nr. 2);
9.2.3. priėmimo – perdavimo aktas (Sutarties priedas Nr. 3).

10. SUTARTIES EGZEMPLIORIAI

10.1. Ši sutartis sudaroma vienu egzemplioriumi, jei pasirašoma elektroniniu parašu arba dviem vienodą teisinę galią turinčiais egzemplioriais – po vieną kiekvienai sutarties šaliai.

11. ŠALIŲ PARAŠAI IR JURIDINIAI REKVIZITAI

Vykdytojas:	**Užsakovas:**
UAB „NBCS“ Įmonės kodas 301817848 PVM mokėtojo kodas LT100006470618 Šeškinės sodų g. 12, LT-08343 Vilnius Tel. +370 5 2764563 El. paštas info@nbcs.lt A/s: LT41 7044 0600 0831 9438, AB „SEB“ Bankas	**Lietuvos Respublikos aplinkos ministerijos Aplinkos projektų valdymo agentūra** Labdarių g. 3 LT-01120 Vilnius Juridinio asmens kodas 288779560 Tel. +370 646 02 285 El. p. apva@apva.lt
Generalinis direktorius	Nacionalinių programų valdymo departamento direktorius, vykdantis direktoriaus funkcijas
Artiom Maslov	Jonas Balkevičius
_____	_____
(parašas)	(parašas)
_____	_____
(data)	(data)

Sutarties priedas Nr. 1

VIEŠOJO PIRKIMO DALYVIO LAIMĖJĘS PASIŪLYMAS
(pateikiamas atskiru dokumentu)

Sutarties priedas Nr. 2

KOMPIUTERINIŲ DARBO VIETŲ BEI TARNYBINIŲ STOČIŲ ANTIVIRUSINĖS APSAUGOS IR KONTROLĖS PROGRAMINĖS ĮRANGOS TURIMŲ LICENCIJŲ PRATĘSIMO PASLAUGŲ PIRKIMO TECHNINĖ SPECIFIKACIJA

Eil. Nr.	Reikalaujami parametrai
1. Bendri reikalavimai	1.1 Siūlomas apsaugos sprendimas turi turėti integruotas sekančias saugumo funkcijas: • antivirusinė sistema apsaugai nuo žalingų programų; • kategorijomis paremta naršymo kontrolė; • išorinių sąsajų kontrolė; • kompiuterinei darbo vietai bei tarnybinėms stotims skirtų ugniasienių valdymas; • aplikacijų kontrolės funkcionalumas; • apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumas; • duomenų nutekėjimo prevencijos kompiuteryje funkcionalumas; • centralizuota saugumo komponentų valdymo konsolė; • apsaugos nuo programinės įrangos klaidos išnaudojimo (angl. exploit prevention); • apsaugos nuo failus užkoduojančių virusų (angl. ransomware prevention) funkcionalumas; • priežasties-pasekmės analizės įrankis (angl. root cause analysis tool); • nurodyto funkcionalumo užtikrinimui gali būti pateikti keli atskiri vieno gamintojo produktai, turintys vieną bendrą visiems produktams skirtą centralizuoto valdymo įrankį.
	1.2 Vienas centralizuoto valdymo įrankis turi galėti valdyti minimaliai šiuos siūlomos programinės įrangos komponentus: • antivirusinė sistema; • naršymo kontrolė; • išorinių kompiuterinės darbo vietos sąsajų kontrolė; • kompiuterinei darbo vietai skirta ugniasienė; • aplikacijų kontrolės funkcionalumas; • apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumas; • duomenų nutekėjimo prevencijos kompiuteryje funkcionalumas;
	1.3 Siūlomas sprendimas turi užtikrinti kompiuterinių darbo vietų apsaugą Windows operacinių sistemų platformoms bei tarnybinių stočių su Windows Server operacinėmis sistemomis nuo 2008 versijos;
	1.4 Siūlomas sprendimo antivirusinė apsauga turi palaikyti virtualias kompiuterines darbo vietas/tarnybines stotis minimaliai šiose platformose (neturi reikalauti atskiros licencijos virtualios infrastruktūros apsaugai): • VMware vSphere / ESX • VMware Worktation • VMware View • Citrix XenServer • Citrix XenApp • Microsoft Hyper-V Server
	1.5 Licencija turi būti skirta apsaugoti ne mažiau nei 130 vartotojų.

	Vartotojui skirta licencija turi apsaugoti daugiau nei vieną kompiuterinį įrenginį (pav. stalinis kompiuteris, nešiojamas kompiuteris, išmanusis mobilus telefonas, planšetinis kompiuteris), t.y. licencijuojama ne per įrenginį. Licencijos galiojimas 24 mėnesiai.
	1.6 Licencija turi būti skirta apsaugoti ne mažiau nei 5 tarnybines stotis. Vartotojų skaičius vienai licencijai turi būti neribotas. Licencijų galiojimas 24 mėnesiai.
2. Reikalavimai antivirusinės sistemos funkcionalumui	2.1 Siūloma sistema turi užtikrinti apsaugą nuo virusų, „spyware“, „adware“, „ransomware“ tipo žalingų programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminų“ ir kitų žalingo tipo programų;
	2.2 Sistema turi galėti proaktyviai blokuoti virusus prieš pasirodant virusų aprašų duomenų bazėms;
	2.3 Sistema turi atlikti žalingų veiksmų stebėseną ir aptikti dar nežinomą žalingą programinę įrangą, tiek prieš paleidžiant/atidarant rinkmeną, tiek po rinkmenos paleidimo turi būti analizuojamas jos elgesys;
	2.4 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.
	2.5 Sistema turi aptikti kenkėjišką internetinį srautą (angl. malicious traffic) į komandų ir kontrolės centrus (angl. command and control center) ir jį blokuoti;
	2.6 Siūlomas sprendimas turi atsinaujinti ne mažiau kaip du kartus per dieną;
	2.7 Sistema turi užtikrinti skenavimą prieigos prie rinkmenų metu ir sistemos krovimosi metu;
	2.8 Sistema turi leisti nustatyti rinkmenų skenavimą kietajame diske pagal iš anksto nustatytus reikalavimus ir turi būti galimybė skirti nurodyta kompiuterio resursų kiekį šiam skenavimui;
	2.9 Siūlomas sprendimas turi galėti automatiškai atlikti sistemos išvalymą nuo aptiktų žalingų programų;
	2.10 Siūloma sistema 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;
	2.11 Sistema turi leisti numatyti išimtis specifinių direktorijų ar rinkmenų skenavimui;
	2.12 Siūloma saugumo sistema turi galėti skenuoti minimaliai šiais standartais archyvuotas rinkmenas: 7z, zip, arj, bzip2, gzip, cab, rar, tar.;
	2.13 Sistema turi gebėti atpažinti failo tipą, t.y. atlikti failo tipo nustatymą ne tik pagal failo tipo plėtinį;
	2.14 Sistema turi užtikrinti saugumą nešiojamiems, staliniams kompiuteriams bei tarnybinėms stotims;
	2.15 Saugumo sistema turi galėti aptikti polimorfines virusų atmainas;
	2.16 Saugumo sistema turi galėti blokuoti įtartinas rinkmenas minimaliai pagal tokius kriterijus: • Naudojamas dvigubas plėtinys; • Rinkmenos plėtinys nesutampa su tikruoju plėtiniu (pav. exe tipo rinkmena yra įvardijama, kaip .txt);
	2.17 Siūloma sistema turi galėti atlikti JavaScript emuliaciją ir elgesio analizę siekiant užtikrinti apsaugą nuo internetu platinamo žalingo kodo;
	2.18 Siūloma apsaugos sistema turi užtikrinti „keliaujančių“ kompiuterių saugų darbą internete, t.y. kai kompiuteris yra ne organizacijos tinkle. Sistema turi gebėti patikrinti interneto svetainės turinį prieš jį pateikiant vartotojo internetinei naršyklei, pagal tokius minimalius parametrus: • Įvertinti ar lankoma svetainė neįeina į infekuotų ir pavojingų tinklalapių sąrašą; • Taikyti svetainių filtravimą pagal kategorijas;
	2.19 Siūlomo sprendimo nustatymų turi būti negalima išjungti eiliniam vartotojui, įskaitant vartotojus turinčius lokalaus administratoriaus teises kompiuteryje;

	2.20 Siūloma saugumo sistema turi palaikyti ir apsaugoti 32/64 bit Windows bei Windows Server 2008 (ir naujesnes) operacines sistemas.
	2.21 Siūloma sistema turi turėti integruotą karantino paskyrą. Administratorius turi galėti leisti prieigą pasirinktiems vartotojams prie jų karantino paskyros, kur vartotojai minimaliai galėtų atlikti šiuos veiksmus: • Išvalyti užkrėstą rinkmeną; • Perkelti užkrėstą rinkmeną; • Ištrinti užkrėstą rinkmeną.
	2.22 Siūlomas produktas informacinių technologijų tyrimo įstaigos Gartner (http://www.gartner.com) duomenimis turi būti tarp lyderiaujančių produktų („Leaders“ kategorijoje) darbo vietų apsaugos platformų grupėje (Magic Quadrant for Endpoint Protection Platforms);
3. Reikalavimai saugumo sistemos centralizuoto valdymo, administravimo ir konfigūravimo funkcijoms	3.1 Siūlomo sprendimo centralizuoto valdymo konsolė turi galėti valdyti apsaugos sistemas Windows platformose.
	3.2 Siūlomo sprendimo atnaujinimas turi galėti vykti tiesiai iš gamintojo atnaujinimo serverio internetu ir turi būti numatyta galimybė kompiuterinėms darbo vietoms parsisiųsti automatiškai atnaujinimus iš lokalaus serverio, kuris prieš tai atnaujinimus gavo iš gamintojo serverio internete;
	3.3 Turi būti galimybė numatyti pirminį ir antrinį atnaujinimo serverius, jei pirminis serveris nepasiekiamas atnaujinimai turi vykti iš antrinio;
	3.5 Siūlomas sprendimas turi leisti nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus sistema išsiųstų el.paštu įspėjimą;
	3.6 Siūlomas sprendimas turi leisti grupuoti, filtruoti ir rūšiuoti apsaugotus kompiuterius centralizuoto valdymo konsolėje minimaliai pagal šiuos parametrus: • Pagal kompiuterio/tarnybinės stoties vardą; • Pagal IP adresą; • Pagal Operacinę sistemą; • Pagal priskirtą vartotoją (Kompiuterinėms darbo vietoms); • Pagal kompiuterio/tarnybinės stoties būklę;
	3.7 Turi būti numatyta 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.
	3.8 Siūlomo sprendimo centralizuoto valdymo konsolė turi integruotis su Active Directory ir veiksmai atliekami direktorijoje turi būti sinchronizuojami su saugumo sprendimo centralizuoto valdymo konsole. Pašalinus vartotoją ar grupę iš Active Directory, tie patys įrašai automatiškai turi būti pašalinami ir iš saugumo sprendimo centralizuoto valdymo konsolės.
	3.9 Siūlomas sprendimas turi leisti taikyti nustatytąją saugumo politiką grupei valdomų kompiuterių/tarnybinių stočių arba individualiems kompiuteriams/tarnybinėms stotims;
	3.10 Siūlomas sprendimas turi leisti rolėmis su skirtingomis administravimo teisėmis paremtą administravimą;
	3.11 Siūlomas sprendimas turi galėti registruoti administratoriaus veiksmus auditavimo tikslais;
	3.12 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;

4.Reikalavimai išorinių serverio sąsajų ir aplikacijų kontrolės funkcionalumui	4.1 Siūlomas sprendimas turi galėti leisti nustatyti kuriems kompiuteriams leidžiama prieiga nustatytiems išoriniams įrenginiams;
	4.2 Siūlomas sprendimas turi galėti kontroliuoti minimaliai šio tipo išorinius įrenginius: • išorinės atminties talpos įrenginius; • CD ir DVD įrenginius; • Floppy įrenginius; • Infraraudonąją jungtimi prijungiamus įrenginius; • Wifi įrenginius; • Bluetooth jungtimi prijungiamas įrenginius.
	4.3 Siūlomas sprendimas turi galėti priskirti išorinio įrenginio naudojimo politiką individualiems kompiuteriams/tarnybinėms stotims ar kompiuterių/tarnybinių stočių grupėms;
	4.4 Siūlomas sprendimas turi galėti 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.
	4.5 Siūlomas sprendimas turi turėti galimybę blokuoti “bridge” režimą tarp laidinio ir bevielio tinklo tame pačiame įrenginyje neprarandant interneto prieigos.
	4.6 Siūlomo sprendimo įrenginių kontrolei pasiekti turi būti valdomas iš tos pačios vartotojo aplinkos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės;
	4.7 Sistema turi leisti kontroliuoti programas (ang. application) 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 panašiai;
	4.8 Sistema turi užtikrinti automatinį kontroliuojamų programų atnaujintų naujomis versijomis aptikimą ir blokavimą;
	4.9 Siūlomas sprendimas turi galėti priskirti aplikacijų naudojimo politiką individualiems kompiuteriams/tarnybinėms stotims ar kompiuterių/tarnybinių stočių grupėms;
	4.10 Siūlomo sprendimo aplikacijų kontrolei pasiekti turi būti valdomas iš tos pačios vartotojo aplinkos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės;
5. Reikalavimai duomenų nutekėjimo prevencijos funkcionalumui (angl. Data loss prevention)	5.1 Siūloma sistema turi turėti integruotą funkcionalumą duomenų iš kompiuterinės darbo vietos/tarnybinės stoties tyčinio ar netyčinio praradimo apsaugai;
	5.2 Sistema turi leisti nustatyti dokumentui žymą (požymį), pagal kurią vėliau būtų atliekama dokumento kontrolė (pav. neleisti su tam tikra žyma dokumento siųsti el.paštu, įkelti per naršyklę išsiuntimui į internetą, kopijuoti į nešifruotą išorinės talpos įrenginį ar persiųsti greitųjų žinučių apsikeitimo programa);
	5.3 Siūlomos sistemos duomenų kontrolės funkcionalumas turi būti valdomas iš tos pačios vartotojo aplinkos („UI“), kaip ir antivirusinė apsauga ir valdomas iš tos pačios centrinio valdymo konsolės;
	5.4 Siūloma sistema turi turėti gamintojo integruotą ir gamintojo atnaujinimą jautrios informacijos duomenų aprašų bazę;
	5.5 Siūloma sistema turi leisti pačiai organizacijai nustatyti turinį kontrolei ir taisykles pasinaudojant nustatymo vedliu;
	5.6 Saugumo sistema turi galėti registruoti veiksmus su kontroliuojamomis rinkmenomis;
	5.7 Saugumo sistema turi galėti leisti nustatyti teisę vartotojui pačiam pasirinkti, kaip elgtis su rinkmena, kurioje yra jautrus turinys. Šie veiksmai turi būti registruojami;
	5.8 Saugumo sistema turi galėti atlikti minimaliai duomenų kontrolę 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.

	5.9 Siūloma sistema turi turėti jau paruoštus šablonus, pagal kuriuos būtų atliekama duomenų nutekėjimo kontrolė;
6. Reikalavimai serverio ugniasienės funkcionalumui	6.1 Siūlomos sistemos klientinė ugniasienė turi būti valdoma centralizuotai iš saugumo sistemos centralizuoto valdymo konsolės;
	6.2 Sistemos ugniasienės nustatymai turėtų būti atliekami naudojant nustatymų vedlį centralizuotai arba lokaliai;
	6.3 Sistemos ugniasienės nustatymo metu turi būti galima naudoti mokymosi režimus (tik stebėti ir rinkti statistiką arba kontroliuoti tinklo profilius);
	6.4 Sistemos ugniasienė turi galėti taikyti skirtingas saugumo nustatymo politikas kompiuteriui esant organizacijos tinkle ir kompiuteriui už organizacijos tinklo perimetro.
	6.5 Sistemos ugniasienės funkcionalumo dalis turi siųsti ataskaitas į centrinę sistemos valdymo konsolę;
7. Reikalavimai tinklalapių filtravimo funkcionalumui	7.1 Siūloma sistema turi turėti galimybę filtruoti internetinius tinklalapius pagal iš anksto sistemoje numatytas kategorijas;
	7.2 Turi būti ne mažiau nei sekančios kategorijos: • Socialinių tinklų • Suaugusiųjų bei potencialiai nepriimtinų svetainių • Didelio pralaidumo reikalaujančių svetainių • Produktyvumą įtakojančių svetainių • Su darbu sisijusių svetainių Aukščiau išvardintos kategorijos turėtu būti toliau detalizuojamos į nemažiau kaip 3 sub-kategorijas kiekvienai kategorijai. Filtravimo politika turi būti nustatoma sistemos centrinėje valdymo konsolėje pagal kompiuterių vartotojų grupes;
	7.3 Turi būti numatyta galimybė įtraukti organizacijos numatytas internetines svetaines ar IP adresus, t.y. susikurti savo filtravimo kategorijas;
	7.4 Sistema turi galėti siųsti informaciją apie blokuotas svetaines į centrinio valdymo konsolę.
	7.5 Siūloma sistema turi realiu laiku blokuoti prieigą prie internetinių tinklalapių kuriuose yra saugomas žalingas kodas;
	7.6 Siūloma sistema turi turėti galimybę apskaičiuoti atsisiunčiamos iš interneto rinkmenos reputaciją prieš ją parsisiunčiant ir pagal tai atitinkamai rekomenduoti arba nerekomenduoti atsisiųsti šią rinkmeną. Reputacija turi būti apskaičiuojama bent pagal šiuos parametrus: rinkmenos paplitimas, atsisiuntimo šaltinis, turinio analizė, rinkmenos senumas.
8. Failų integralumo tarnybinėje stotyje stebėjimas	8.1 Kritinių Windows operacinės sistemos failų pakeitimų stebėjimas ir prevencija. 8.2 Galimybė nustatyti papildomas stebėjimo lokacijas / katalogus. 8.3 Galimybė nustatyti išimtis.
9. Tarnybinėje stotyje įdiegtų programų stebėjimas, naujų diegimų draudimas	9.1 Galimybė automatiškai išanalizuoti serveryje įdiegtas programas bei sukurti „baltajį sąrašą“ (angl.: whitelist). 9.2 Galimybė uždrausti programų neesančių baltajame sąraše diegimą ar paleidimą. 9.3 Galimybė laikinai pridėti papildomą progamą į baltajį sąrašą neatjungiant bendro draudimo.
10. Palaikymas	10.1 Turi būti užtikrintas siūlomos saugumo programinės įrangos atnaujinimas, virusų aprašų ir kitų duomenų bazių atnaujinimas 12 mėnesių.
	10.2 Turi būti teikiama programinės įrangos gamintojo techninio palaikymo paslauga 24 valandas per parą, septynias dienas per savaitę 24 mėnesių laikotarpiui.
11. Kitos sąlygos	11.1 Licencijos pratęsimo kaina nurodoma taip: … eurų / 2 metams / vnt. 11.2 Licencijų pratęsimo terminas įsigalioja nuo 2021 m. rugsėjo 17 d. 11.3 Tiekėjas apie užsakytų licencijų įjungimą informuoja el. paštu itskyrius@apva.lt. 11.4 Apmokėjimas už prekes atliekamas per 30 (trisdešimt) dienų nuo PVM sąskaitos-faktūros gavimo dienos.

	11.5 Paslaugų teikėjas sąskaitas ir priėmimo – perdavimo aktus privalo teikti naudojantis “E. Sąskaita” sistema www.esaskaita.eu.

Sutarties priedas Nr. 3

PRIĖMIMO – PERDAVIMO AKTAS

20__ m. _____ d.

Lietuvos Respublikos aplinkos ministerijos Aplinkos projektų valdymo agentūra, toliau vadinama UŽSAKOVU, ir **UAB „NBCS“,** atstovaujami direktoriaus Artiom Maslov, toliau vadinamas VYKDYTOJU, sudaro šį aktą:

1. UŽSAKOVAS priėmė iš VYKDYTOJO dalį jo suteiktų Prekių pagal 2021 m. d. sutarties Nr. APVA/2021/08/10 1.1 punktą. Kita dalis bus priimama atskiru aktu.
2. UŽSAKOVAS patvirtina, kad perduodama dalis Prekių atitinka šalių sutartus reikalavimus ir sutarties sąlygas.
3. Laikotarpiu nuo 20__ m. _____ d. iki 20__ m. _____ d. VYKDYTOJAS pateikė pagal sutartį:
   3.1. Prekes <*įrašyti prekių pavadinimą*>.
4. VYKDYTOJO suteiktų Prekių vertė yra _____ Eur (_____).
5. UŽSAKOVAS sumokės VYKDYTOJUI _____ Eur per 30 dienų nuo PVM sąskaitos faktūros, išrašytos pagal šį priėmimo – perdavimo aktą, gavimo dienos.
6. PVM sąskaitą faktūrą UŽSAKOVUI pateikia VYKDYTOJAS.
7. UŽSAKOVAS ir VYKDYTOJAS pareiškia, kad neturi jokių pretenzijų vienas kitam, išskyrus UŽSAKOVO prievolę sumokėti VYKDYTOJUI pagal šį aktą.

UŽSAKOVAS:

Lietuvos Respublikos aplinkos ministerijos Aplinkos projektų valdymo agentūra

Labdarių g. 3 LT-01120 Vilnius
Juridinio asmens kodas 288779560
Tel. +370 646 02 285
El. p. apva@apva.lt

VYKDYTOJAS:

UAB „NBCS“

Įmonės kodas 301817848
PVM mokėtojo kodas LT100006470618
Šeškinės sodų g. 12, LT-08343 Vilnius
Tel. +370 5 2764563
El. paštas info@nbcs.lt
A/s: LT41 7044 0600 0831 9438, AB „SEB“ Bankas

Generalinis direktorius
Artiom Maslov

Lietuvos Respublikos aplinkos ministerijos
Aplinkos projektų valdymo agentūrai
(adresatas (perkančioji organizacija))

PASIŪLYMAS
DĖL KOMPIUTERINIŲ DARBO VIETŲ BEI TARNYBINIŲ STOČIŲ ANTIVIRUSINĖS APSAUGOS IR KONTROLĖS PROGRAMINĖS ĮRANGOS TURIMŲ LICENCIJŲ PRATĘSIMO PASLAUGŲ PIRKIMO

2021-08-06
(Data)
Vilnius

Tiekėjo pavadinimas	UAB NBCS
Tiekėjo adresas	Šeškinės sodų g. 12, Vilnius
Tiekėjo įmonės kodas	301817848
Tiekėjo banko sąskaitos Nr./bankas	LT41 7044 0600 0831 9438; AB „SEB“ Bankas
Už pasiūlymą atsakingo asmens vardas, pavardė	Vilma Gricukė
Telefono numeris	868263485
Fakso numeris	-
El. pašto adresas	vilma.gricuke@nbcs.lt

Šiuo pasiūlymu pažymime, kad sutinkame su visomis pirkimo sąlygomis, nustatytomis:
1) techninėje specifikacijoje;
2) kituose pirkimo dokumentuose (paaiškinimuose, papildymuose).

Siūlome licencijas šiomis kainomis:

Eil. Nr.	Pirkimo objektas	Licencijos pavadinimas	Mato vienetas	Kiekis	Kaina, EUR be PVM
	1	*2*	*3*	*4*	*5*
1.	Kompiuterinių darbo vietų antivirusinės apsaugos ir kontrolės programinės įrangos licencijos 24 mėn. laikotarpiui	Central Intercept X Endpoint Advanced	vnt.	130	7020,00
2.	Tarnybinių stočių antivirusinės apsaugos ir kontrolės programinės įrangos licencijos 24 mėn. laikotarpiui	Central Intercept X Advanced for Server	vnt.	5	890,00
				Bendra kaina, Eur be PVM:	7910,00
				PVM suma, Eur:	1661,10
				Bendra kaina, Eur su PVM:	9571,10

Siūlomos licencijos visiškai atitinka techninėje specifikacijoje nurodytus reikalavimus ir jų savybes.

Pasiūlymas galioja 60 (šešiasdešimt) dienų.

Vilma Gricukė

(Tiekėjo arba jo įgalioto asmens vardas, pavardė, parašas)

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Aplinkos projektų valdymo agentūra, Labdariu g. 3
Dokumento pavadinimas (antraštė)	Sutartis su UAB „NBCS“ dėl licencijų Nr. APVA/2021/08/10
Dokumento registracijos data ir numeris	2021-08-11 Nr. (29-2-7)-S-212
Dokumento gavimo data ir dokumento gavimo registracijos numeris	2021-08-17 10:31:22 Nr. G-2704
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0, GEDOC
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	JONAS BALKEVIČIUS, DEPARTAMENTO DIREKTORIUS
Parašo sukūrimo data ir laikas	2021-08-11 07:13:34
Parašo formatas	Parašas, pažymėtas laiko žyma
Laiko žymoje nurodytas laikas	2021-08-11 07:13:44
Informacija apie sertifikavimo paslaugų teikėją	ADIC CA-B
Sertifikato galiojimo laikas	2020-04-01 - 2023-04-01
Parašo paskirtis	Registravimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Kristina Burbaitė, ADMINISTRATORĖ
Parašo sukūrimo data ir laikas	2021-08-11 08:21:56
Parašo formatas	Trumpalaikis skaitmeninis parašas, kuriame taip pat saugoma sertifikato informacija
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	RCSC IssuingCA
Sertifikato galiojimo laikas	2021-01-07 - 2023-01-07
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Artiom Maslov, Generalinis direktorius
Parašo sukūrimo data ir laikas	2021-08-11 10:47:52
Parašo formatas	Trumpalaikis skaitmeninis parašas, kuriame taip pat saugoma sertifikato informacija
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016
Sertifikato galiojimo laikas	2019-10-01 - 2024-09-29
Parašo paskirtis	Gauto dokumento registravimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Kristina Burbaitė, ADMINISTRATORĖ
Parašo sukūrimo data ir laikas	2021-08-17 10:31:22
Parašo formatas	Trumpalaikis skaitmeninis parašas, kuriame taip pat saugoma sertifikato informacija
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	RCSC IssuingCA

Sertifikato galiojimo laikas	2021-01-07 - 2023-01-07
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	0
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Elektroninė dokumentų valdymo sistema VDVIS, versija v. 3.04.02
El. dokumento įvykius aprašantys metaduomenys	
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	El. dokumentas atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja. Tikrinimo data: 2021-08-17 14:39:35
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2021-08-17 atspausdino Juozas Marčinskas
Paieškos nuoroda	