

SUTARTIS Nr. APVA/2019/08/28

Vilnius,

data 2019-08-28

UAB „NBCS“, įmonės kodas 301817848, atstovaujama direktoriaus Artiom Maslov (toliau – **Vykdytojas**) ir Lietuvos Respublikos aplinkos ministerijos Aplinkos projektų valdymo agentūra, atstovaujama direktoriaus pavaduotojo Vytauto Vrubliausko, pavaduojančio direktorių pagal Lietuvos Respublikos aplinkos ministerijos Aplinkos projektų valdymo agentūros 2019 m. rugpjūčio 12 d. pavedimą Nr. P1-29 (toliau – **Užsakovas**), sudarė šią sutartį (toliau – sutartis):

1. SUTARTIES DALYKAS

1.1. Vykdytojas įsipareigoja pagal techninėje specifikacijoje (Sutarties priedas Techninė specifikacija) pateiktas technines charakteristikas Užsakovui išnuomoti Kompiuterinių darbo vietų apsaugos ir kontrolės programinės įrangos metines licencijas (toliau – Licencijos), o Užsakovas įsipareigoja sumokėti už Licencijas šioje Sutartyje nustatyta tvarka.

2. PRISTATYMO TVARKA IR TERMINAI

2.1. Tiekėjas Licencijas turi pristatyti ne vėliau kaip iki 2019-09-28 (el. paštu ir/ar kt. būdu).

2.2. Vykdytojas Licencijas turi pristatyti el. paštu andrius.lukosiunas@apva.lt.

3. ATSISKAITYMŲ TVARKA

3.1. Užsakovas už programinės įrangos metinių licencijų nuomą sumoka Vykdytojui pagal šiuos įkainius:

Eil. Nr.	Pavadinimas	Mato vienetas	Maksimalus kiekis	Vieneto kaina Eur, be PVM	Suma Eur, be PVM
1.	Vartotojų skaičius, kuriuos turi apsaugoti licencija (Sophos Central Intercept X Advanced)	vnt.	120	36,29	4354,8
2.	Serverių skaičius, kuriuos turi apsaugoti licencija (Sophos Central Intercept X Advanced for Server)	vnt.	16	91,30	1460,8
Bendra kaina Eur, be PVM:					5815,60
PVM 21%:					1221,28
Bendra kaina Eur, su PVM:					7036,88

3.2. Į Licencijų kainą privalo būti įskaičiuotos visos su Licencijų nuoma susijusios išlaidos.

3.3. Vykdytojas, už Licencijų nuomą, 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. Išnuomoti Licencijas šioje Sutartyje nustatytais 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. Išsinuomoti Licencijas;
- 4.3.2. sumokėti už jas nustatytą kainą Sutartyje numatytais sąlygomis ir tvarka.
- 4.4. Užsakovas turi teisę:
- 4.4.1. reikalauti pristatyti nuomojamas Licencijas;
- 4.4.2. pareikalauti atlyginti nuostolius, jeigu Vykdytojas, pažeisdamas Sutartį, neišnuomoja (nepateikia) Licencijų Užsakovui Sutartyje numatytais terminais ir tvarka.
- 4.5. Jei Vykdytojas Sutartyje nustatytais terminais neišnuomoja Licencijų, tai jis sumoka delspinigius, kurie lygūs 0,02 % (dvi šimtosios procento) nuo neišnuomotų Licencijų kainos už kiekvieną pradelstą dieną.
- 4.6. Jei Užsakovas per šios Sutarties 3.4. 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 nesuteikia 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 pasirašymo dienos ir galioja 12 (dvylika) mėnesių.
- 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 prieš 5 (penkias) kalendorines dienas.

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. techninė specifikacija (Sutarties priedas Nr. 1);

9.2.2. priėmimo – perdavimo aktas (Sutarties priedas Nr. 2).

10. SUTARTIES EGZEMPLIORIAI

10.1. Ši sutartis sudaroma dviem vienodą teisinę galią turinčiais egzemplioriais – po vieną kiekvienai sutarties šaliai.

8. ŠALIŲ PARAŠAI IR JURIDINIAI REKVIZITAI

Vykdytojas:

UAB „NBCS“

Įmonės kodas 301817848

PVM mokėtojo kodas LT100006470618

J.Kazlauskio g. 21 LT-08314 Vilnius, Lietuva

Tel. +370 5 2764563

El. paštas info@nbcs.lt

A/s: LT83 7290 0000 1346 7076

AB „Citadele“ Bankas

Užsakovas:

Lietuvos Respublikos aplinkos ministerijos

Aplinkos projektų valdymo agentūra

Įstaigos kodas 288779560

Labdarių g. 3, LT-01120 Vilnius

Tel. 272 5758, faksas 272 2563

apva@apva.lt

Direktorius
Artiom Maslov

Direktoriaus pavaduotojas, pavaduojantis
direktorių
Vytautas Vrubliauskas



*Vyriausiasis specialistas
vidinių pirkimų specialisto
asistentas*

Juozas Marčinskas

2019-08-28



*Tėsinis šlypian
kyšiančioji specialiste*

Ernesta Jonkambaitė



*Finansų kontrolės skyriaus
patarėja
Irina Nikolajeva*



*Vyriausiasis specialistas
Andrius Lukošius*



TECHNINĖ SPECIFIKACIJA

Kompiuterinių darbo vietų apsaugos ir kontrolės programinė įranga:

Eil. Nr.	Reikalaujami parametrai
Kompiuterinių darbo vietų apsaugos ir kontrolės sprendimas	
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 kompiuterinės darbo vietos sąsajų kontrolė; • kompiuterinei darbo vietai skirta ugniasienės 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 antivirusinę apsaugą Windows bei Mac operacinių sistemų platformoms;
	1.4 Siūlomas sprendimo antivirusinė apsauga turi palaikyti virtualias kompiuterines darbo vietas/tarnybines stotis minimaliai šiose platformose (neturi reikalausti atskiros licencijos virtualios infrastruktūros apsaugai): • VMware vSphere / ESX • VMware Workstation • VMware View • Citrix XenServer • Citrix XenApp • Microsoft Hyper-V Server
	1.5 Licencija turi būti skirta apsaugoti ne mažiau nei 120 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 12 mėnesių.
2. Reikalavimai antivirusinės sistemos funkcionalumui	2.1 Siūloma sistema turi užtikrinti apsaugą nuo virusų, „spyware“, „adware“, „ransomware“ tipo žalingų programų, „rootkits“, potencialiai nepageidaujamų aplikacijų, „kirminių“ 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 naršyklės (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 direktorių ar rinkmenų skenavimui;
	2.12 Siūloma saugumo sistema turi galėti skenuoti minimaliai šiais standartais archyvuotas rinkmenas: 7z, zip, arj, bzip2, gzip, MS 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 terminalinėms 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 64 bit macOS 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) 2018 metų 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 bei Mac platformose.
	3.2 Siūlomo sprendimo kompiuterinių darbo vietų atnaujinimas turi galėti vykdyti 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, tam, kad jei kompiuterinė darbo vieta yra lokaliame tinkle ji siunčiasi atnaujinimus iš lokalaus atnaujinimų serverio (pirminis serveris), jei ta pati darbo vieta naudojama už organizacijos tinklo perimetro ribų, atnaujinimus ji turi galėti parsisiųsti iš gamintojo serverio internetu arba iš serverio patalpinto organizacijos DMZ zonoje (antrinis serveris);
	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 vardą; • Pagal IP adresą; • Pagal Operacinę sistemą; • Pagal priskirtą vartotoją;

	• Pagal kompiuterio būklę;
	3.7 Turi būti numatyta galimybė sistemos administratoriui nuotoliniu būdu išspręsti problemas pasirenkant vieną ar keletą kompiuterių „vienu mygtuko paspaudimu“ šiems veiksams: • Apsaugoti kompiuterį įdiegiant ar pakartotinai įdiegiant apsaugos programinę įrangą; • Priverstinai paleisti atnaujinimą; • Paleisti pilną sistemos skenavimą; • Pašalinti įspėjamuosius pranešimus; • Priverstinai pritaikyti nustatytą 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 nustatytą saugumo politiką grupei valdomų kompiuterių arba individualiems kompiuteriams;
	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 prijungiamus įrenginius.
	4.3 Siūlomas sprendimas turi galėti priskirti išorinio įrenginio naudojimo politiką individualiems kompiuteriams ar kompiuterių 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), greitujų žinučių apsikeitimo programos (pav. Skype), žaidimai ir panašiai;
	4.8 Sistema turi užtikrinti automatinį kontroliuojamų programų atnaujinimų naujomis versijomis aptikimą ir blokavimą;
	4.9 Siūlomas sprendimas turi galėti priskirti aplikacijų naudojimo politiką individualiems kompiuteriams ar kompiuterių 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 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 greitujų 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 nepriimtinių svetainių • Didelio pralaidumo reikalaujančių svetainių • Produktyvumą įtakančių svetainių • Su darbu susijusių svetainių Aukščiau išvardintos kategorijos turėtų 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, atsisisiuntimo šaltinis, turinio analizė, rinkmenos senumas.
8. Palaikymas	8.1 Turi būti užtikrintas siūlomos saugumo programinės įrangos atnaujinimas, virusų aprašų ir kitų duomenų bazių atnaujinimas 12 mėnesių.
	8.2 Turi būti teikiama programinės įrangos gamintojo techninio palaikymo paslauga 24 valandas per parą, septynias dienas per savaitę 12 mėnesių laikotarpiui.

Serverių apsaugos ir kontrolės programinė įranga:

Eil. Nr.	Reikalaujami parametrai
Serverių apsaugos ir kontrolės sprendimas	
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; • serverio ugniasienės valdymas; • aplikacijų kontrolės funkcionalumas; • apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumas; • duomenų nutekėjimo prevencijos 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 sąsajų kontrolė; • serverio ugniasienės valdymas; • aplikacijų kontrolės funkcionalumas; • apsaugos nuo Interneto grėsmių ir filtravimo funkcionalumas; • duomenų nutekėjimo prevencijos kompiuteryje funkcionalumas; 1.3 Siūlomas sprendimas turi užtikrinti antivirusinę apsaugą Windows Server operacinėms sistemoms nuo 2008 versijos; 1.4 Siūloma sprendimo antivirusinė apsauga turi palaikyti virtualiserverius minimaliai šiose platformose (neturi reikalauti atskiros licencijos virtualios infrastruktūros apsaugai): • VMware vSphere / ESX • VMware Workstation • VMware View

	• Microsoft Hyper-V Server
	1.5 Licencija turi būti skirta apsaugoti ne mažiau nei 16 serverių. Vartotojų skaičius vienai licenzijai turi būti neribotas. Licencijos galiojimas 12 mėnesių.
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 naršyklės (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 direktorių ar rinkmenų skenavimui;
	2.12 Siūloma saugumo sistema turi galėti skenuoti minimaliai šiais standartais archyvuotas rinkmenas: 7z, zip, arj, bzip2, gzip, MS 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 Saugumo sistema turi galėti aptikti polimorfines virusų atmainas;
	2.15 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);
	2.16 Siūloma sistema turi galėti atlikti JavaScript emuliaciją ir elgesio analizę siekiant užtikrinti apsaugą nuo internetu platinamo žalingo kodo;
	2.17 Siūlomo sprendimo nustatymų turi būti negalima išjungti eiliniam vartotojui, įskaitant vartotojus turinčius lokalaus administratoriaus teises kompiuteryje;

	2.18 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.
	2.19 Siūlomas produktas informacinių technologijų tyrimo įstaigos Gartner (http://www.gartner.com) 2018 metų 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 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;
	3.2 Turi būti galimybė numatyti pirminį ir antrinį atnaujinimo serverius, jei pirminis serveris nepasiekiamas atnaujinimai turi vykti iš antrinio.
	3.3 Siūlomas sprendimas turi leisti nustatyti įspėjamuosius ir kritinius lygius, kuriuos pasiekus sistema išsiųstų el.paštu įspėjimą;
	3.4 Siūlomas sprendimas turi leisti grupuoti, filtruoti ir rūšiuoti apsaugotus serverius centralizuoto valdymo konsolėje minimaliai pagal šiuos parametrus: • Pagal kompiuterio vardą; • Pagal IP adresą; • Pagal Operacinę sistemą; • Pagal serverio būklę;
	3.5 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.
	3.6 Siūlomas sprendimas turi leisti taikyti nustatytą saugumo politiką grupei valdomų serverių arba individualiems serveriams;
	3.7 Siūlomas sprendimas turi leisti rolėmis su skirtingomis administravimo teisėmis paremtą administravimą;
	3.8 Siūlomas sprendimas turi galėti registruoti administratoriaus veiksmus auditavimo tikslais;
	3.9 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 serveriams 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 serveriams ar serverių 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 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;
	4.6 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;
	4.7 Sistema turi užtikrinti automatinį kontroliuojamų programų atnaujinimą naujomis versijomis aptikimą ir blokadimą;
	4.8 Siūlomas sprendimas turi galėti priskirti aplikacijų naudojimo politiką individualiems serveriams ar serverių grupėms;
	4.9 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 serverio 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 („UT“), 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 taisyklės 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/jkeliant 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 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 nepriimtinių svetainių • Didelio pralaidumo reikalaujančių svetainių • Produktyvumą įtakančių svetainių • Su darbu susijusių svetainių Aukščiau išvardintos kategorijos turėtų 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 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. Serveryje įdiegtų programų stebėjimas, naujų diegimų draudimas	9.1 Galimybė automatiškai išanalizuoti serveryje įdiegtas programas bei sukurti „baltąjį sąrašą“ (angl.: whitelist). 9.2 Galimybė uždrausti programų neesančių baltajame sąraše diegimą ar paleidimą. 9.3 Galimybė laikinai pridėti papildomą programą į baltąjį 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 12 mėnesių laikotarpiui.

PRIĖMIMO – PERDAVIMO AKTAS

20__ m. _____ d.

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

1. UŽSAKOVAS priėmė iš VYKDYTOJO dalį jo suteiktų Paslaugų pagal 2019 m. rugpjūčio 28 d. sutarties Nr. APVA/2019/08/28 1.1 punktą. Kita dalis bus priimama atskiru aktu.
2. UŽSAKOVAS patvirtina, kad perduodama dalis Paslaugų atitinka šalių sutartus reikalavimus ir sutarties sąlygas.
3. Laikotarpiu nuo 20__ m. _____ d. iki 20__ m. _____ d. VYKDYTOJAS suteikė pagal sutartį:
3.1. Paslaugas <įrašyti paslaugų pavadinimą>.
4. VYKDYTOJO suteiktų Paslaugų 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
Įstaigos kodas 288779560
Labdarių g. 3, LT-01120 Vilnius
Tel. 272 5758, faksas 272 2563
apva@apva.lt

VYKDYTOJAS:

UAB „NBCS“
Įmonės kodas 301817848
PVM mokėtojo kodas LT100006470618
J.Kazlauskio g. 21 LT-08314 Vilnius, Lietuva
Tel. +370 5 2764563
El. paštas info@nbcs.lt
A/s: LT83 7290 0000 1346 7076
AB „Citadele“ Bankas

Direktorius
Artiom Maslov

Vyriausiasis specialistas
vidinių pirkimų specialisto
asistentas
Juozas Marčinskas