SUTARTIS NR. APVA/2021/01/25

2021 m. sausio 25 d., Vilnius

Lietuvos Respublikos aplinkos ministerijos Aplinkos projektų valdymo agentūra (toliau – **Užsakovas**), atstovaujama direktoriaus Ignoto Šalavėjaus, veikiančio pagal įstaigos nuostatus ir

UAB „NBCS“ (toliau – **Vykdytojas**), atstovaujama generalinio direktoriaus Artiom Maslov, veikiančio pagal įmonės įstatus,

toliau kartu ar atskirai vadinami Šalimis, sudarė šią pirkimo – pardavimo sutartį (toliau – Sutartis).

1. SUTARTIES DALYKAS

1.1. Vykdytojas įsipareigoja pagal techninėje specifikacijoje (Sutarties priedas Nr. 1. Techninė specifikacija) pateiktą aprašymą suteikti aukšto patikimumo tinklo ugniasienių sprendimo paslaugas (toliau – Paslaugos), o Užsakovas įsipareigoja apmokėti už Paslaugas šioje sutartyje nustatyta tvarka.

2. PASLAUGŲ TEIKIMO TVARKA

2.1. Paslaugų teikimo tvarka turi atitikti techninėje specifikacijoje nurodytą tvarką.
2.2. Vykdytojas įsipareigoja užtikrinti, kad Migravimo iš senos ugniasienės į naują sprendimą paslaugos ir naujo sprendimo palaikymo (garantijos) paslaugos visu palaikymo (garantijos) laikotarpiu bus teikiamos pagal įdiegtą informacijos saugumo valdymo sistemą, atitinkančią LST ISO/IEC 27001 standarto reikalavimus arba lygiavertes informacijos saugumo valdymo priemones, ir pateikti tai įrodančius dokumentus.
2.3. Užsakovas įsipareigoja suteikti visą reikiamą informaciją, esančią jo dispozicijoje, kuri gali būti svarbi Sutarties vykdymui.
2.4. Visa vykdant Sutartį Vykdytojo parengta dokumentacija yra Užsakovo nuosavybė ir Užsakovas turi teisę ją skelbti be Vykdytojo sutikimo.

3. ATSISKAITYMŲ TVARKA

3.1. Užsakovas už faktiškai suteiktas aukšto patikimumo tinklo ugniasienių sprendimo paslaugas sumoka Vykdytojui pagal šias kainas:

Eil. Nr.	**Pirkimo objektas**	**Mato vienetas**	**Kiekis**	**Vieneto kaina EUR be PVM**	**Kaina EUR be PVM** *(4x5)*
1	*2*	*3*	*4*	*5*	*6*
1.	Dviejų vienetų ugniasienių klasteris	Vnt.	1	2 045,00	2 045,00
2.	Ugniasienių programinė įranga 3 metų laikotarpiui	Vnt.	1	7 288,00	7 288,00
3.	Migravimo iš senos ugniasienės į naują sprendimą paslaugos	Vnt.	1	1 182,00	1 182,00
	Pasiūlymo kaina EUR be PVM (6 stulpelio reikšmių suma)				10 515,00
	PVM *(pildoma, jei taikoma*				2 208,15
	Pasiūlymo kaina EUR su PVM				12 723,15

3.2. Numatomi du mokėjimai Vykdytojui už suteiktas paslaugas:
3.2.1. Už suteiktus Dviejų vienetų ugniasienių klasterį ir Ugniasienių programinę įrangą 3 metų laikotarpiui.

3.2.2. Už suteiktas Migravimo iš senos ugniasienės į naują sprendimą paslaugas.
3.3. Suteikęs Sutartyje numatytas Paslaugas Vykdytojas Užsakovui pateikia Paslaugų priėmimo – perdavimo aktą (Sutarties priedas Nr. 2. Paslaugų priėmimo – perdavimo aktas).
3.4. Abiem šalims pasirašius Paslaugų priėmimo – perdavimo aktą, Vykdytojas Užsakovui pateikia PVM sąskaitą faktūrą, kurią Užsakovas apmoka per 30 (trisdešimt) kalendorinių dienų nuo jos gavimo dienos. PVM sąskaitos faktūros ir priėmimo – perdavimo aktai privalo būti teikiami naudojantis "E.sąskaita" sistema www.esaskaita.eu.

4. ŠALIŲ ATSAKOMYBĖ

4.1. Jeigu Vykdytojas nukrypsta nuo Sutarties sąlygų ir suteikia netinkamos kokybės Paslaugas arba jeigu Vykdytojas padaro darbe kitokių trūkumų, Užsakovas turi teisę reikalauti neatlygintinai ištaisyti nurodytus trūkumus per nurodytą terminą.
4.2. Vykdytojo teikiamose Paslaugose nustačius esminių nukrypimų nuo Sutarties sąlygų ar kitokių esminių trūkumų, Užsakovas turi teisę reikalauti nutraukti sutartį ir atlyginti nuostolius.
4.3. Jei Vykdytojas nustatytais terminais nesuteikia numatytų Paslaugų, tai jis sumoka delspinigius, kurie lygūs 0,02 % (dvi šimtosios procento) nuo nesuteiktų Paslaugų vertės už kiekvieną pradelstą dieną.
4.4. Jei Užsakovas per šios Sutarties 3.3 punkte nurodytą terminą neatsiskaito su Vykdytoju, jis Vykdytojui privalo sumokėti 0,02 % (dvi šimtosios procento) dydžio delspinigius nuo nesumokėtos sumos už kiekvieną uždelstą dieną.
4.5. Jei Vykdytojas su Užsakovu suderintais terminais neatlieka numatytų Paslaugų ir vėluoja daugiau kaip 14 dienų, tai jis sumoka Užsakovui baudą, kurios dydis apskaičiuojamas sumažinant Paslaugų kainą 30 proc. ir atitinkamą sumą išskaičiuojant iš Užsakovui apmokėjimui pateiktos PVM sąskaitos-faktūros. Baudos išskaičiavimas neatleidžia Vykdytojo nuo prievolės įvykdymo.

5. FORCE MAJEURE

5.1. 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.
5.2. Nustatant force majeure aplinkybes, taikomos Lietuvos Respublikos Vyriausybės 1996 07 15 nutarimo Nr. 840 nuostatos.

6. SUTARTIES GALIOJIMAS

6.1. Sutartis įsigalioja nuo pasirašymo momento ir galioja iki 2021 m. gegužės 31 d.
6.2. Sutartis gali būti nutraukta raštišku abiejų šalių susitarimu arba vienos šalies iniciatyva Sutartyje ar Lietuvos Respublikos teisės aktuose numatytais pagrindais.
6.3. Kiekviena šalis gali vienašališkai nutraukti šią Sutartį prieš tai raštu pranešusi kitai Šaliai ne mažiau kaip prieš 30 (trisdešimt) kalendorinių dienų.
6.4. Sutarties nutraukimas bet kokiais pagrindais neatleidžia šalių nuo prievolių sumokėti visas sumas, kurios tapo mokėtinomis iki Sutarties nutraukimo.

7. TAIKYTINA TEISĖ IR GINČŲ SPRENDIMAS

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

8. SUTARTIES PRIEDAI IR KEITIMAS

8.1. Sutarties sąlygos sutarties galiojimo laikotarpiu negali būti keičiamos, išskyrus tokias sutarties sąlygas, kurias pakeitus nebūtų pažeisti Viešųjų pirkimų įstatymo nustatyti pagrindiniai principai ir tikslai.
8.2. Visi sutarties priedai laikomi neatskiriama jos dalimi:

8.2.1. techninė specifikacija (Sutarties priedas Nr. 1);
8.2.2. priėmimo – perdavimo aktas (Sutarties priedas Nr. 2).

9. SUTARTIES EGZEMPLIORIAI

9.1. Ši sutartis sudaroma dviem vienodą teisinę galią turinčiais egzemplioriais – po vieną kiekvienai sutarties šaliai, jei sutartis pasirašoma elektroniniu parašu - sudaromas vienas sutarties egzempliorius.

8. ŠALIŲ PARAŠAI IR JURIDINIAI REKVIZITAI

Vykdytojas:

UAB „NBCS“

Įmonės kodas 301817848
PVM mokėtojo kodas LT100006470618
J.Kazlausko g. 21 LT-08314 Vilnius
Tel. +370 5 2764563
El. paštas info@nbcs.lt
A/s: LT41 7044 0600 0831 9438
AB „SEB“ Bankas

Generalinis direktorius
Artiom Maslov

_____
(parašas)
_____
(data)

(A.V.)

Užsakovas:

Lietuvos Respublikos aplinkos ministerijos
Aplinkos projektų valdymo agentūra
Labdarių g. 3 LT-01120 Vilnius
Juridinio asmens kodas 288779560
Tel. 8 646 02 285
El. p. apva@apva.lt

Direktorius
Ignotas Šalavėjus

_____
(parašas)
_____
(data)

(A.V.)

Sutarties priedas Nr. 1

TECHNINĖ SPECIFIKACIJA

I. PIRKIMO TIKSLAS

1.1. Užtikrinti APVA saugumo politikos reikalavimų įgyvendinimą, bei turimos tinklo ugniasienės, kurios 2021 m. II ketv. baigsis gamintojo palaikymas, atnaujinimą.

II. PIRKIMO OBJEKTAS

2.1. Aukšto patikimumo tinklo ugniasienių sprendimas su migravimo paslaugomis iš senos ugniasienės į naują sprendimą.

III. PIRKIMO OBJEKTO SUDĖTIS

3.1. Aukšto patikimumo tinklo ugniasienių sprendimas (dviejų ugniasienių klasteris su reikalingomis programinės įrangos, reikalingos užtikrinti ugniasienių funkcionalumą, licencijomis 3 metų laikotarpiui).
3.2. Migravimo paslaugos iš senos ugniasienės į naują sprendimą.

IV. PLANUOJAMAS ĮSIGYTI KIEKIS

4.1. Aukšto patikimumo tinklo ugniasienių sprendimas (1 komplektas) – pristatomas per 4 savaites nuo sutarties pasirašymo.
4.2. Migravimo paslaugos iš senos ugniasienės į naują sprendimą – įgyvendinimo terminas iki 2021-04-30.

V. TECHNINIAI REIKALAVIMAI

5.1. Reikalavimai fizinėms sąsajoms.

5.1.1. Aukšto patikimumo tinklo ugniasienių sprendimą turi sudaryti ne mažiau kaip 2 vnt. tinklo ugniasienių, veikiančių aktyvus - pasyvus režime, kai tik vienas įrenginys praleidžia srautą vienu metu, o rezervinis įrenginys naudojamas tik sugedus pirmajam. Aukšto patikimumo tinklo ugniasienių sprendimas turi būti sudarytas iš to paties gamintojo techninės ir programinės įrangos. Siūlomame sprendime turi būti sukomplektuota visa tam reikalinga techninė įranga ir programinės įrangos licencijos (3 metų laikotarpiui) pagal reikalavimus pateiktus žemiau.
5.1.2. Reikalavimai fizinių sąsajų skaičiui (kiekviename ugniasienės įrenginyje):
ne mažiau 6 x 1GBE vario prievadų;
ne mažiau 2 x GBE SFP prievadų;
ne mažiau 3 x USB 3.0;
ne mažiau 1 x COM (RJ45).
5.1.3. Integruotas, ne mažesnis kaip 120 GB SDD diskas, skirtas vietiniam karantinui, talpyklai (cache) bei ataskaitoms (logs).
5.1.4. Įrenginiai montuojami į standartinę 19 colių spintą, kiekvieno ne daugiau kaip 1U aukštis. Montavimo dalys pridedamos.
5.1.5. Integruotas maitinimo šaltinis 100-240 VAC, 50-60 Hz.

5.2. Reikalavimai tinklo srauto apdorojimo pajėgumams.

5.2.1. Ugniasienės pralaidumas ne mažiau 32 Gbps.
5.2.2. Virtualaus privataus tinklo prieigos vartų pralaidumas ne mažiau 2 Gbps.
5.2.3. Apsaugos nuo įsiveržimo (IPS) pralaidumas ne mažiau 4,8 Gbps.
5.2.4. Next-Generation Ugniasienės (IPS, interneto turinio ir aplikacijų kontrolės) pralaidumas ne mažiau 9 Gbps.
5.2.5. TCP konkurencinių prisijungimų skaičius ne mažiau kaip 6,5 milijonų.
5.2.6. TCP naujų sesijų per sekundę ne mažiau 100 tūkstančių.

5.2.7. Ugniasienės našumas turi atitikti organizacijos techninius reikalavimus, bei turi būti gamintojo rekomenduojamas ne mažiau kaip 200 vartotojų tinklui, ne mažiau kaip 300 Mbps interneto pralaidumui bei 200 nuotolinių darbuotojų.

5.3. Valdymo ir aukšto patikimumo reikalavimai.

5.3.1. Valdymas turi būti paremtas internetine naršykle be papildomos programinės įrangos įdiegimo. Komunikacija turi būti šifruojama per HTTPS.

5.3.2. Turi būti galimybė sukurti kelis vartotojus įrenginio valdymui (administrator accounts).

5.3.3. Galimybė naudoti dviejų faktorių autentifikavimą administratoriams, vartotojų savitarnos portalui bei VPN prisijungimams.

5.3.4. Administravimas turi būti paremtas rolėmis su galimybe kurti savo roles. Galimybė sukurti rolę kuriai leidžiama tik peržiūrėti parametrus, bet neleidžiama jų keisti.

5.3.5. Turi būti galimybė keliems administratoriams prisijungti bei daryti pakeitimus vienu metu.

5.3.6. Administratoriaus vartotojas turi būti automatiškai atjungiamas (log off) po tam tikro neveiksnumo (idle) laiko.

5.3.7. Turi būti galimybė įrenginį valdyti per API, kad būtų galima sujungti su trečiųjų šalių įrankiais.

5.3.8. Turi būti galimybė valdyti įrenginį per komandinę eilutę.

5.3.9. Turi būti galimybė daryti atsargines nustatymų kopijas lokaliai, į FTP, į e-mail / rankiniu būtų, kas dieną, kas savaitę, kas mėnesį. Turi būti galimybė užkoduoti atsargines kopijas su administratoriaus pasirinktu slaptažodžiu.

5.3.10. Administravimo įrankyje turi būti galimybė klonuoti objektus.

5.3.11. Turi būti patogūs trikčių šalinimo įrankiai, tokie kaip registro peržiūra (log viewer), paketų surinkimas (packet capture), ugniasienės taisyklių tikrinimas.

5.3.12. Visi atnaujinimai turi būti pateikiami iš sprendimo gamintojo.

5.3.13. Atnaujinimai turėtų būti atsiunčiami automatiškai ir laikomi saugumo sistemoje integruotame diske. Taip pat turi būti galimybė atnaujinimus diegti iš USB atmintinės jei įrenginys neturi interneto prieigos.

5.3.14. Šablonų aprašymų atnaujinimai turi būti atsiunčiami ir įdiegiami automatiškai.

5.3.15. „Firmware“ ir aprašų šablonų įkėlimas gali būti atliekamas pagal iš anksto sudarytą grafiką.

5.3.16. Turi būti siunčiami automatiniai pranešimai apie atsiradusią naują „firmware“ versiją.

5.3.17. Turi būti galimybė grąžinti ankstesnę „firmware“ versiją per grafinę vartotojo sąsają perkrovus įrenginį, bet ne perrašant operacinės sistemos.

5.3.18. Turi būti galimybė matyti konfigūracijos pakeitimus.

5.4. Reikalavimai ugniasienės paketų filtravimui ir maršrutizavimui.

5.4.1. Išsamus paketų inspektavimas (angl. „deep packet inspection“).

5.4.2. Paketų filtras paremtas prievadais ir zonomis.

5.4.3. NAT (angl. Network Address Translation) maskavimas.

5.4.4. PAT (angl. Port Address Translation).

5.4.5. SNAT (angl. Source Network Address Translation).

5.4.6. DNAT (angl. Destination Network Address Translation).

5.4.7. Pilnas NAT (angl. FullNAT).

5.4.8. NAT išimtys (angl. NoNAT).

5.4.9. 1:1 NAT (Network Address Translation).

5.4.10. IP ir MAC adresais paremtas filtravimas.

5.4.11. Turi palaikyti kelių prievadų sugrupavimą (angl. link aggregation) pagrįstą 802.3ad standartu.

5.4.12. Registrų įjungimas/išjungimas taisyklei.

5.4.13. Aprašymas/įvardinimas kompiuterių, tinklų ir servisų.

5.4.14. Turi galėti apjungti objektus į grupes.

5.4.15. Turi būti integruotos sistemos registrai/ataskaitos, taip pat registras taisyklių taikymo aktyvumui.

5.4.16. Turi palaikyti statinį ir dinaminį maršrutizavimą (RIP, BGP, OSPF).

5.4.17. Turi palaikyti nepriklausomų grupinio transliavimo protokolų maršrutizavimą.

5.4.18. Turi palaikyti VLAN žymėjimą.
5.4.19. Galimybė blokuoti pagal kilmės šalį (valstybę):
galimybė nurodyti blokuojamos šalies srauto kryptį (įeinančiam/išeinančiam) srautui;
nustatomos išimtys.
5.4.20. Turi būti integruota naujos kartos ugniasienės technologija leidžianti filtruoti remiantis aplikacija/paslauga:
turi būti galima daryti išimtis remiantis vartotoju/IP/ tinklu;
atpažįstamų aplikacijų duomenų bazę turi sudaryti ne mažiau nei 3000 aplikacijų;
naujų aplikacijų aprašai turi būti atnaujinami automatiškai;
dinaminis aplikacijų blokavimas remiantis rizikos klase ir produktyvumo indeksacija.
5.4.21. DHCP palaikymas:
turi būti integruotas DHCP serveris;
statinis išdavimas (static lease);
turi būti integruotas DHCP persiuntimas (angl. relay).
5.4.22. Interneto prievadų (WAN) balansavimo reikalavimai:
turi automatiškai balansuoti srautą tarp kelių interneto prievadų.
turi būti įdiegtas interneto prievadų diagnozavimo mechanizmas.
sugedus pagrindiniam interneto prievadui turi automatiškai persijungti į atsarginę interneto liniją.
5.4.23. Reikalavimai SD-WAN funkcijoms:
turi būti galimybė nukreipti srautą pagal įeinantį prievadą, srauto ištakos (source) ir tikslo (destination) adresą, servisą (prievadą), aplikaciją, vartotoją ar vartotojų grupę;
turi būti galimybė aprašyti kaip nukreipti srautą jeigu sugenda pagrindinė linija bei kai ji vėl pradeda veikti naudojant įvairias sujungimo technologijų kombinacijas (pvz.: MPLS, VPN, DSL);
SD-WAN funkcijos turi būti palaikomos tiek su IPv4 tiek IPv6;
turi būti galimybė valdyti kokia tvarka maršrutizatorius peržiūri VPN, statinio bei SD-WAN maršrutizavimo taisykles.

5.5. Srauto prioritizavimo ir valdymo reikalavimai.

5.5.1. Galimybė prioritizuoti (Quality of Service) srautą pagal kompiuterį, servisą bei vartotoją.
5.5.2. Galimybė vartotojams nustatyti persiunčiamų duomenų kvotas. Bendra kvota ir arba periodinė kvota.
5.5.3. Galimybė taikyti VoIP optimizacijas.
5.5.4. Galimybė naudoti DSCP žymes.

5.6. Reikalavimai vartotojų autentifikavimui.

5.6.1. Vietiniai vartotojai (valdomi ir laikomi saugumo sistemoje).
5.6.2. Turi palaikyti šiuos autentikavimo metodus:
RADIUS;
TACACS;
LDAP;
eDirectory.
5.6.3. Turi palaikyti skaidrų tarpinės tarnybinės stoties autentikavimą (NTLM ir Kerberos) arba autentikavimą su kompiuteryje įdiegtu agentu.
5.6.4. Turi turėti autentikavimo agentus šioms operacinėms sistemoms:
Windows;
Mac OS X;
Linux 32/64.
5.6.5. Galimybė naudoti kelis autentifikacijos būdus paraleliai, pavyzdžiui kelis Active Directory serverius.
5.6.6. Reikalavimai vartotojų autentifikacija skaidriame rėžime:
Active Directory SSO;
Autentifikacija vietiniame portale.

5.6.7. Turi turėti vienkartinių slaptažodžių funkcionalumą (angl. OTP) per RADIUS/TACACS/LDAP (išoriniai) arba per integruota (vidini). Reikalavimai vidinei OTP funkcijai:
vienkartinio slaptažodžio aplikacija (angl. OTP) skirta Android ir iOS;
turi būti be papildomos licencijos išoriniam OTP serveriui;
turi būti galimybė pradinius nustatymus atlikti per savitarnos portalą;
turi palaikyti trečių šalių fizinius OTP įrenginius.
5.6.8. Vienkartinių slaptažodžių funkcionalumas turi veikti su šiomis įrenginio funkcijomis:
IPSec nuotolinė prieiga;
SSL VPN;
vartotojų savitarnos portalas;
administratoriaus WEB konsolė.
5.6.9. Google Chromebook autentifikavimo palaikymas kai naudojama Active Directory ir Google Gsuite.
5.7. Turi būti vartotojų savitarnos portalas, kuris minimaliai galėtų atlikti šiuos veiksmus:
parsisiųsti VPN prieigos klientą ir jo konfigūracinį failą;
sužinoti WiFi prieigos informaciją;
pakeisti vartotojo slaptažodį;
patikrinti asmeninę interneto naršymo ataskaitą;
peržiūrėti elektroninio pašto žinutes esančias karantine;
susikonfigūruoti dviejų faktorių autentifikaciją su QR kodu.
5.8. Reikalavimai SSL / TLS srauto dekodavimui.
5.8.1. Galimybė nenaudojant proxy dešifruoti bet kokį SSL / TLS srautą (ne tik HTTPS).
5.8.2. Galimybė dešifruoti TLS 1.3 srautą nežeminant TLS versijos į 1.2 ar žemesnę.
5.8.3. Galimybė kurti lankčias dešifravimo taisykles pagal:
srauto ištakos (source) zoną arba adresą;
srauto tikslo (destination) zoną, adresą arba servisą / prievadą;
vartotoją arba vartotojų grupę;
Internetinio puslapio kategoriją ir/arba adresą.
5.8.4. Galimybė pasirinkti, ką daryti su srautu kurio neįmanoma dešifruoti: leisti, atmesti, nukirsti (allow, reject, drop).
5.9. Reikalavimai virtualaus privataus tinklo technologijai.
5.9.1. Turi palaikyti Cisco klientus.
5.9.2. PPTP prisijungimas (Client-to-Site architektūroje).
5.9.3. L2TP per IPSec prisijungimas (Client-to-Site architektūroje).
5.9.4. Turi palaikyti Windows IPSec Tunnel modulį.
5.9.5. Reikalavimai standartiniams IPSec prisijungimams „Site-to-Site“ architektūroje:
IPSec tunelio aprašymas keliems vietiniams/nutolusiems tinklams;
„Site-to-Site“ VPN galimybė tarp dviejų sistemų turinčių dinaminius IP abiejose pusėse.
5.9.6. Turi palaikyti NAT-Traversal funkcionalumą.
5.9.7. Turi būti palaikomi šie šifravimo algoritmai:
DES bei 3DES;
AES/Rijndael (128, 192 bei 256 Bit);
SHA1 bei SHA2 (256, 384, 512 Bit);
DH Grupės 1,2,5,14;
Blowfish bei TwoFish;
Serpent;
MD5.
5.9.8. SSL VPN prisijungimai (Client-to-Site architektūroje):
turi dirbti su tarpinėmis tarnybinėmis stotimis ir NAT maršrutizatoriais;
turi galėti priskirti kliento IP iš adresų sąrašo (pool);

tunelio modulis (galimybė naudoti visus intraneto servisus).
5.9.9. SSL VPN prisijungimai (Site-to-Site architektūroje):
turi dirbti su tarpinėmis tarnybinėmis stotimis ir NAT maršrutizatoriais;
turi priskirti kliento IP iš adresų sąrašo (pool);
tunelio modulis (galimybė naudoti visus intraneto servisus);
prisijungimai į abi kryptis.

5.10. Reikalavimai integruotoms saugumo sistemoje ataskaitoms bei registrui ir įspėjimo pranešimams.

5.10.1. Įvykių žurnalai turi būti kaupiami įrenginyje.
5.10.2. Turi būti pateikiama grafinė informacija apie įrangą (CPU, kietąjį diską, tinklą ir kitus parametrus).
5.10.3. Turi būti pateikiama grafinė informacija apie vartotojų interneto vartojimą (persiųstų MB kiekį, top siuntėjai, top puslapiai) ir tinklo utilizaciją.
5.10.4. Ataskaitų informacijos anonimizavimo (maskavimo) galimybė (el.pašto) (vartotojo vardas/IP adresas, pašto domenas ir pašto adresai turėtų būti uždengiami). Atrakinimas šios informacijos turėtų vykti dviejų slaptažodžių pagalba.
5.10.5. Galimybė eksportuoti ataskaitas HTML, PDF, Excel (XLS) formatais.
5.10.6. Registras turi būti galimas keliuose išoriniuose Syslog serveriuose.
5.10.7. Registras centriniame ataskaitų serveryje.
5.10.8. Atskiri registrų failai skirtingiems moduliams.
5.10.9. Įspėjimo pranešimas per SNMP Trap (SNMPv2 ir SNMPv3 palaikymas).

5.11. Reikalavimai įsiveržimo aptikimo ir prevencijos sistemai (IPS).

5.11.1. Turi būti integruota apsauga nuo atsisakymo aptarnauti atakų (angl. DoS).
5.11.2. Rankinis pavienių atakų išjungimas.
5.11.3. Galimybė nustatyti apsaugą remiantis pagal atakas į operacines sistemas.
5.11.4. Galimybė nustatyti išimtis IDS taisyklių taikymui tinklams ir kompiuteriams.
5.11.5. Anomalijų aptikimas (apsauga nuo nulinės dienos atakų).
5.11.6. Prievadų skanavimo aptikimas.
5.11.7. Atskiri registrų lygiai IDS ir IPS dalims.
5.11.8. Turi būti integruota apsauga nuo komunikacijos su žalingomis valdymo tarnybinėmis stotimis (angl. Botnet command and control server).
5.11.9. Turi būti automatiniai šablonų atnaujinimai.
5.11.10. Sistema turi galėti aptikti pažengusius pavojus, tokius, kaip botnet tinklai ar komandų ir kontrolės serverius, keliais mechanizmais (minimaliai ugniasienės, DNS, IPS, web proxy).
5.11.11. SYN Flood aptikimas:
turi būti numatyta galimybė daryti išimtis;
registrai;
Syn Flood normos reguliavimas;
pagal šaltinį (source)/ paskirtį (destination)/ maišytas nustatymas.
5.11.12. UDP Flood aptikimas:
turi būti numatyta galimybė daryti išimtis;
registrai;
UDP Flood normos reguliavimas;
pagal šaltinį (source) / paskirtį (destination)/ maišytas nustatymas.
5.11.13. ICMP Flood aptikimas:
turi būti numatyta galimybė daryti išimtis;
registrai;
ICMP Flood normos reguliavimas;
pagal šaltinį (source) / paskirtį (destination)/ maišytas nustatymas.

5.12. Reikalavimai VPN veikiančiam per naršyklę:

turi palaikyti beklientį VPN:
turi veikti naršyklės pagrindu;
turi nereikalauti įskiepių (plugin), naršyklės priedėlių (add-on), papildomų aplikacijų;
turi palaikyti RDP, VNC, Telnet, SSH, HTTP/S protokolus.

5.13. Reikalavimai interneto turinio saugumo funkcionalumui.

5.13.1. Turi būti galimos išimtys šaltinio IP/Tinklams.
5.13.2. Maksimalus skenuojamo failo dydis nustatomas pagal poreikį.
5.13.3. Web turinio filtro praleidimas pagal poreikį (blokuojamiems URL).
5.13.4. Turi būti integruoti nemažiau nei du virusų skenavimo varikliai su skirtingomis virusų aprašų bazėmis. Turi būti galimybė naudoti abu skenavimo variklius tuo pačiu metu.
5.13.5. Pirminės tarpinės tarnybinės stoties palaikymas:
vartotojų autentifikacija pirminėje tarpinėje tarnybinėje stotyje;
neribotas pirminių tarpinių tarnybinių stočių skaičius;
pirminės tarpinės tarnybinės stoties pasirinkimas remiantis tokiais parametrais, kaip šaltinio IP, vartotojas/grupė vartotojų, laikas, domenas, URL.
5.13.6. HTTP tarpinės tarnybinės stoties PAC failų talpinimas:
Auto-config kliento per DHCP;
Auto-config kliento per DNS.
5.13.7. Antivirusinė apsauga skirta:
HTTP atsiuntimams;
HTTPS atsisiuntimams;
FTP atsisiuntimams (per naršyklę);
FTP atsisiuntimams (komandinė eilutė/FTP klientas) (skaidrus FTP tarpinės tarnybinės stoties).
5.13.8. Skirtingų saugumo profilių konfigūravimas:
atskyrimas paremtas vietine autentifikacija;
atskyrimas paremtas LDAP direktorija;
atskyrimas paremtas AD SSO;
atskyrimas paremtas eDirectory SSO;
atskyrimas paremtas tinklu (vartotojo IP adresas);
autentifikacija per RADIUS;
autentifikacija per TACACS+.
5.13.9. Reikalavimai filtravimui ir blokavimui:
pagal URL kategorijas;
pagal baltą sąrašą;
pagal juodą sąrašą;
pagal Java/JavaScript/ActiveX;
MIME tipo tikrinimas proxy apžiūra (magic lookup);
pagal failų plėtinius (.exe, .gif, …);
pagal MIME dokumentų tipą (iš serverio);
turi būti integruota šnipinėjimo programinę įranga aptinkanti sistema (turi tikrinti įeinantį srautą ir “skambinimą namo” (išeinantį) srautą);
pagal potencialiai nepageidaujamą aplikaciją;
remiantis aplikacijų lygiu (L7 ugniasienė);
pagal nežinomą (neįtrauktas į kategoriją) tinklalapį;
filtravimas paremtas laiko parametru arba diena.
5.13.10. URL filtro funkcionalumo reikalavimai:
kategorijų grupės neribotos;
reputacija paremtas URL blokavimas;
leisti/blokuoti kategorijas remiantis laiko parametru arba diena;

turi būti daugiau nei 90 skirtingų kategorijų;
URL duomenų bazės užklausos realiu laiku (nėra poreikio duomenų bazės atnaujinimams);
URL filtras juodo sąrašo rėžime (viskas leidžiama išskyrus nepasirinktas kategorijas) arba balto sąrašo rėžimas (viską blokuoti išskyrus pasirinktas kategorijas);
pasirenkamos išimtys remiantis tokiais parametrais, kaip: Šaltinis/Tikslas/Domenas/Serveris/ Kategorija.

5.14. Reikalavimai elektroninio pašto saugumo funkcionalumui.

5.14.1. Turi būti:
SMTP prieigos vartų rėžimas;
skaidrus rėžimas (MX įrašo konfigūravimas nėra būtinas);
el.pašto persiuntimas su „round robin“;
SMTP autentifikacija (el. paštas priimamas tik tada jei vartotojas yra autentifikuotas);
antivirusinė apsauga skirta SMTP, POP3, IMAP;
2 ar daugiau integruoti skirtingų gamintojų virusų aprašų bazės;
gaunančiųjų domenų skaičius neribotas;
Antispam apsauga SMTP, POP3, IMAP srautui;
neturi būti licencinių apribojimų konkurenciniams el. pašto prisijungimams.
5.14.2. Reikalavimai Anti-SPAM apsaugai:
galimi filtro veiksmai “Ištrinti”, “Įspėti”, “Ignoruoti” ir “Karantinuoti”;
galimybė keisti pridedamą žymę “SPAM” el. pašto pavadinimo laukelyje;
Anti-Spam siuntėjų globalus baltas sąrašas;
Anti-Spam siuntėjo baltas sąrašas kiekvienam el. pašto gavėjui (nustatomas pačio vartotojo);
Anti-Spam siuntėjo juodas sąrašas kiekvienam el. pašto gavėjui (nustatomas pačio vartotojo);
Juodi/Balti sąrašai gali būti keičiami administratoriaus.

VI. REIKALAVIMAI ĮRANGOS ATNAUJINIMUI, GARANTIJAI, UGNIASIENIŲ MIGRAVIMO PASLAUGOMS

6.1. Techninei įrangai suteikiama ne mažiau kaip 3 metų gamintojo garantija. Techninės įrangos gedimo atveju gamintojas turi išsiųsti naują techninę įrangą pakeitimui ne vėliau kaip per 24 valandas po gamintojo patvirtinimo dėl techninės įrangos pakeitimo.
6.2. Programinės įrangos, saugumo modulių (kurie turi būti periodiškai atnaujinami), virusų duomenų bazės atnaujinimai internetu turi būti užtikrinti ne mažiau kaip 3 metus. Teisė diegtis gamintojo paskelbtas naujausias programinės įrangos versijas, gauti gamintojo išleidžiamus atnaujinimus, gauti gamintojo išleidžiamus pagerinimus į naujas versijas ir tiesioginį gamintojo palaikymą.
6.3. Turi būti užtikrintas ne prastesnis kaip 24 val. per parą, 7 dienos per savaitę tiesioginis gamintojo techninis palaikymas (telefonu, el. paštu).
6.4. Aukšto patikimumo sprendimas privalo būti sumontuotas ir paruoštas darbui perkančiosios organizacijos serverinėje, bei turi būti pilnai atlikti migracijos ir diegimo darbai nuo esamų ugniasienių (organizacijoje naudojamas Cyberoam CR50iNG su Total Value licencija), įskaitant visų pagal licenciją naudojamų funkcijų bei politikų perkėlimą ir sukonfigūravimą.
6.5. Turi būti pateikti oficialūs gamintojo nuotoliniai apmokymai ugniasienės administravimui ne mažiau kaip dviem organizacijos specialistams.

VII. KITOS SĄLYGOS

7.1. Sutarties galiojimo trukmė – iki 2021 metų gegužės 31 d. (imtinai).
7.2. Apmokėjimas už prekes ir paslaugas atliekamas per 30 (trisdešimt) dienų nuo PVM sąskaitos-faktūros (sąskaitų faktūrų) gavimo dienos.
7.3. Paslaugų teikėjas sąskaitas privalo teikti naudojantis “E. sąskaita” sistema www.esaskaita.eu.

Sutarties priedas Nr. 2

PRIĖMIMO – PERDAVIMO AKTAS

20__ m. _____ d.

Lietuvos Respublikos aplinkos ministerijos Aplinkos projektų valdymo agentūra, atstovaujama _____, toliau vadinama UŽSAKOVU, ir **UAB „NBCS“,** atstovaujama _____, toliau vadinama VYKDYTOJU, sudaro šį aktą:

1. UŽSAKOVAS priėmė iš VYKDYTOJO dalį jo suteiktų Paslaugų pagal 2021 m. sausio 25 d. sutarties Nr. APVA/2021/01/25 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.

Vykdytojas:	**Užsakovas:**
UAB „NBCS“ Įmonės kodas 301817848 PVM mokėtojo kodas LT100006470618 J.Kazlausko g. 21 LT-08314 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 Juridinio asmens kodas 288779560 El. p. apva@apva.lt Direktorius Ignotas Šalavėjus
_____	_____
(parašas)	**(parašas)**
_____	_____
(data)	**(data)**

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Aplinkos projektų valdymo agentūra, Labdariu g. 3
Dokumento pavadinimas (antraštė)	Sutartis su UAB "NBCS" Nr. APVA/2021/01/25
Dokumento registracijos data ir numeris	2021-01-25 Nr. (29-2-7)-S-21
Dokumento gavimo data ir dokumento gavimo registracijos numeris	2021-01-26 19:28:28 Nr. G-332
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0, GEDOC
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	IGNOTAS ŠALAVĖJUS, Direktorius
Parašo sukūrimo data ir laikas	2021-01-23 16:26:04
Parašo formatas	Trumpalaikis skaitmeninis parašas, kuriame taip pat saugoma sertifikato informacija
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	ADIC CA-B
Sertifikato galiojimo laikas	2021-01-05 - 2024-01-05
Parašo paskirtis	Registravimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Kristina Burbaitė, ADMINISTRATORĖ
Parašo sukūrimo data ir laikas	2021-01-25 09:44:51
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	2021-01-26 14:45:05
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	2021-01-26 19:28:29
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	0
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: 2021-01-27 08:21:44
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2021-01-27 atspausdino Remigijus Plakys
Paieškos nuoroda	