ACHIZIŢII PUBLICE

CONTRACT nr. 34-03/16
de achiziţionare a bunurilor

Cod CPV: 48220000-6

"30" noiembrie 2016 **mun. Chişinău**

SC „Reţele Terestre" SRL (IDNO) 1007600026075, în persoana Directorului **dnul Victor CIOCLEA,** care acţionează în baza statutului, denumit în continuare „Vînzător" pe de o parte, şi

Serviciul Stare Civilă, (IDNO) 1008601000400, în persoana Directorului adjunct **dna Veronica BUSUIOC-VOLOSATÎI**, acţionând în baza Ordinului Ministerului Justiţiei, nr. 374-c din 21 noiembrie 2016, numit în continuare **„Cumpărător"**, pe de altă parte, ambii denumiţi în continuare *Părţi*, au încheiat prezentul Contract referitor la următoarele:

1. **Achiziţionarea software-ului Antivirus pentru anii 2016-2019**, denumit în continuare Bunuri, în baza deciziei Grupului de lucru pentru achiziţii publice al Cumpărătorului expusă în Procesul verbal nr. 65/16 din 22.11.2016.

2. Următoarele documente vor fi considerate părţi componente şi integrale ale Contractului:

a) Specificaţia tehnică şi preţ (anexa nr.1, parte integrantă a prezentului contract);
b) Caracteristicile tehnice (anexa nr. 2 la contract).

3. Prezentul Contract va predomina asupra tuturor altor documente componente. În cazul unor discrepanţe sau inconsecvenţe între documentele componente ale Contractului, documentele vor avea ordinea de prioritate enumerată mai sus.

4. În calitate de contravaloare a plăţilor care urmează a fi efectuate de Cumpărător, Vînzătorul se obligă prin prezenta să livreze Cumpărătorului Bunurile şi să înlăture defectele lor în conformitate cu prevederile Contractului sub toate aspectele.

5. Cumpărătorul se obligă prin prezenta să plătească Vînzătorului, în calitate de contravaloare a livrării bunurilor, precum şi a înlăturării defectelor lor, preţul Contractului sau orice altă sumă care poate deveni plătibilă conform prevederilor Contractului în termenele şi modalitatea stabilite de Contract.

Digitally signed by Cioclea Victor
Date: 2020.11.30 09:18:03 EET
Reason: MoldSign Signature
Location: Moldova

11.7. Persoana responsabilă de executarea prezentului contract din partea SSC este dl Alexandr GUȚAL Șef al Secției gestionarea echipamentului tehnic și programare DSISC tel. 022 25-72-05, iar din partea Vînzătorului _____ dna(ul)_____, tel_____

11.8. Prezentul Contract reprezintă acordul de voință al ambelor părți și este semnat astăzi, "29" noiembrie 2016 .

Pentru confirmarea celor menționate mai sus, Părțile au semnat prezentul Contract în conformitate cu legislația Republicii Moldova, la data și anul indicate mai sus.

Datele juridice, poștale și bancare ale Părților:

Vînzătorul:

SC „Rețele Terestre" S.R.L.
str. Mitropolit G.Bănulescu Bodoni, nr. 45,
mun. Chișinău
c/f 1007600026075
BC „Mobiasbanca"SA
fil. 2, Rîșcani
MOBBMD22
MD96MO2224ASV36891807100
Tel: 022101777/022101777

Director
Victor CIOCLEA _____

Cumpărătorul:

Serviciul Stare Civilă
Str. M.Viteazul, 11/1, mun. Chișinău
c/f 1008601000400
Ministerul Finanțelor,
Trezoreria de Stat, TREZMD2X
MD34TRPBAA317110A00827AE
E 397200,00
Tel. 257125, 257205

Director
Veronica BUSUIOC-VOLOSATÎI _____

2016-00000 18974

TREZORERIA TERITORIALĂ CHIȘINĂU BUGETUL DE STAT
REPUBLICA MOLDOVA, MINISTERUL FINANȚELOR
TREZORERIA TERITORIALĂ CHIȘINĂU
BUGETUL DE STAT
13. DEC. 2016 6
Nr. de înregistrare
Contract
Semnătura

Contabil
Înregistrat: nr._____
Trezoreria_____
_____
"___"_____

Anexa nr.1
Contract nr. 34-03/16

Specificație tehnică și preț

Nr	Denumirea bunului procurat	Cod CPV	Cantitatea/set	Preț totală fără TVA	Preț total cu TVA
1	Software Antivirus pentru anii 2016-2019	*48220000-6*	1 set (include 600 tilizatori (36 luni), cu administrare centralizată și 60 servere (36 luni))	[redacted]	[redacted]

Vînzătorul:

SC „Rețele Terestre" S.R.L.

Director
Victor CIOCLEA _____

Cumpărătorul:

Serviciul Stare Civilă

Director adjunct
Veronica BUSUIOC-VOLOSATÎI _____

Anexa nr. 2
La contractul nr. 34-05/16

CARACTERISTICI GENERALE ALE PRODUSULUI

Produsul trebuie sa fie o platforma integrata pentru managementul securitatii, gîndită ca o solutie modulara formata din urmatoarele module:

A. O consola de management care asigura functionalitati de administrare.
B. Protecție antimalware pentru statii fizice, laptop-uri si servere.
C. Protectie antimalware pentru medii virtualizate.
D. Protectie si securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android.
E. Controlul dispozitivelor, controlul accesului la Internet, filtrarea traficului prin modul de tip firewall pentru masinile fizice si virtuale.
F. Protectie si securitate pentru serverele email Microsoft Exchange

A. CONSOLA DE MANAGEMENT

1. Instalare si configurare:

1. Pachetul de instalare va fi livrat ca o masina virtuala bazata pe sistem de operare Linux securizat care contine toate rolurile sau serviciile necesare. Imaginea de tip template se va putea importa in:
   a. VMware vSphere
   b. Citrix XenServer
   c. Microsoft Hyper-V
   d. Red Hat Enterprise Virtualization
   e. KVM
   f. Oracle VM.
2. Solutia va fi scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe masini virtuale sau pe aceeasi masina virtuala.
3. Masinile de scanare pentru mediile virtuale VMware si Citrix se insteaza la distanta prin task din consola de management, iar pentru alte platforme se descarca separat din interfata web a produsului.
4. Rolurile principale trebuie sa fie cel putin similare cu: Server cu baza de date, Server de comunicatie, Server de actualizare, Server de Web.
5. Solutia va include aditional si un modul de balansare (load balancer) pentru cazurile in care mai multe masini virtuale ale componentei de management sunt instalate cu acelasi rol (pentru Load Balancing si performanta).
6. Solutia va include un mecanism de configurare a disponibilitatii pentru Serverul cu baze de date.

2. Cerinte generale:

1. Solutia va include un modul de update server prin care se asigura actualizarea de produs si a semnaturilor.
2. Solutia va pemite activarea/dezactivarea actualizarilor de produs/semnaturi.
3. Notificarile – prezente in interfata, notificarile necitite sunt evidentiate, trimise catre una sau mai multe adrese de email, alerteaza administratorul in cazul unor probleme majore: licentiere, detectie virusi, actualizari de produs disponibile).
4. Solutia va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware.
5. Solutia va permite instalarea serviciului de SMNP prin care se pot raporta statusul masinilor din cadrul componentei de management.

3. Panou de monitorizare si raportare (Dashboard):

1. Rapoartele din panoul de monitorizare vor putea fi configurate specificand numele raportului, tipul raportului, tinta raportului, optiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul dupa care o statie este considerata neactualizata).
2. Panoul central contine rapoarte pentru toate modulele suportate.
3. Rapoartele din panoul central de comanda permit: adaugarea altor rapoarte, stergerea lor si rearanjarea.

4. Inventarierea retelei – managementul securitatii:

1. Solutia se va integra cu Active Directory, VMware vCenter, Citrix Xen si importa inventarul acestor platforme.
2. Pentru integrarea cu Active Directory, se va putea defini si intervalul (in ore) de sincronizare si forta sincronizarea.
3. Se permite descoperirea masinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.
4. Se permite descoperirea statiilor statii fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery.
5. Solutia va oferi optiuni de cautare, sortare si filtrare dupa numele sistemului, sistem de operare si adresa IP.
6. Solutia va permite instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale.
7. Solutia va permite selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale.
8. Solutia va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware.
9. Solutia va oferi posibilitatea de repornire a masinilor fizice de la distanta.

10. Solutia va oferi informatii detaliate despre fiecare task si se fiseaza daca task-ul s-a finalizat sau nu cu succes.
11. Solutia va permite configurarea centralizata a clientilor antimalware prin intermediul politicilor
12. Se vor oferi in consola de management informatii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnaturi.

5. Politici:

1. Solutia va permite configurarea setarilor antimalware prin intermediul politicilor din consola de magement.
2. Politica va contine optiuni specifice de activare/dezactivare si configurarea functionalitatilor precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicatiilor, scanarea traficului web,controlul dispozitivelor, power user.
3. Solutia permite aplicarea politicilor pe masini client, grupuri de masini, pool-uri de resourse (VMware), domeniu, unitati organizationale.

6. Rapoarte:

1. Solutia va contine rapoarte care prezinta statusul masinilor clientil din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate.
2. Rapoartele programate pot fi trimise catre un numar nelimitat de adrese de email (nu este nevoie sa aiba un cont in consola de management).
3. Solutia va permite vizualizarea rapoartelor curente programate de administrator.
4. Solutia va permite exportarea rapoartelor in format .pdf si detaliile ca format .csv.

7. Carantina:

1. Solutia va permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila.
2. Permite descarcarea fisierelor carantinate doar pentru masinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield.

8. Utilizatori:

1. Administrarea se va putea face pe baza de roluri.
2. Roluri multiple predefinite: Administrator companie, Administrator retea, Reporter sau rol personalizat.
   a. Administrator companie: administreaza arhitectura consolei de management;
   b. Administrator retea: administreaza serviciile de securitate;
   c. Reporter: monitorizeaza si genereaza rapoarte.

3. Utilizatorii pot fi importati din Microsoft Active Directory sau creati in consola de management.
4. Se va permite configurarea detaliata a drepturilor administrative, permitand selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari.
5. Se va permite deconectarea automata a oricarui tip de utilizator dupa un anumit timp pentru o protectie sporita a datelor afisate in consola de administrare. Acest interval se poate personaliza de administratorul solutiei.

9. Log-uri:

1. Inregistrarea actiunilor utilizatorilor.
2. Se vor oferi informatii detaliate pentru fiecare actiune a unui utilizator.
3. Se va permite filtrarea actiunilor utilizator dupa numele utilizatorului, actiune.

10. Actualizare:

1. Se permite definirea de locatii de actualizare multiple.
2. Se permite activarea/dezactivarea actualizarilor de produs si semnaturi.
3. Se permite actualizarea produsului intr-o retea fara acces la Internet.

10. Certificate:

1. Accesul la consola de management sa se faca prin HTTPS.
2. Serverul web, din consola centrala de management trebuie sa permita importarea de certificate digitale eliberate de o autoritate de certificare autorizata sau proprie organizatiei.
3. Solutia permite afisarea in consola de management informatii despre certificate: nume, autoritatea emitenta, data eliberarii si data expirarii certificatelor eliberate.

B. PROTECTIE STATII SI SERVERE FIZICE/VIRTUALE

1. Caracteristici generale minimale si eliminatorii:

1. Existenta unui singur motor de scanare, pentru a nu se incarca suplimentar memoria sistemelor de calcul.
2. Pentru reducerea la minim a consumului de resurse, solutia antimalware trebuie sa permita instalarea personalizata a modulelor detinute (de exemplu, sa permita instalarea solutiei antimalware fara modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall).

2. Cerinte de sistem:

- Sisteme de operare pentru statii de lucru: Windows 10, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3), Mavericks (10.9.x), Mountain Lion (10.8.x), Lion (10.7.x)
- Sisteme de operare embedded: Windows Embedded10, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded

Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7, Windows Embedded POSReady 2009, Windows Embedded Standard 2009, Windows XP Embedded with Service Pack 2, Windows XP Tablet PC Edition

- Sisteme de operare pentru servere: Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server
- Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual and Debian 5.0 sau mai recent.

3. Administrare si instalare remote:

1. Inainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
2. Instalarea se va putea face in mai multe moduri:
    a. prin descarcarea directa a pachetului pe statia pe care se va face instalarea;
    b. prin instalarea la distanta, direct din consola de management
3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui client existent in locatiile respective de tip relay pentru a minimiza traficul in WAN.
4. In consola vor fi disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc.
5. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere.
6. Consola va include o sectiune, „Audit", unde se vor mentiona toate actiunile intreprinse fie de administratori fie de reporteri, cu informatii detaliate: logare, editare, creare, delogare, mutare etc.
7. Posibilitatea creari unui singur pachet de instalare, utilizabil atat pentru sistemele de operare pe 32 de biti cat si pentru cele pe 64 de biti.
8. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
9. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu.

10. Permite selectarea clientului care va realiza descoperirea statiilor din retea, altele decat cele integrate in domeniu.

4. Caracteristici si functionalitati principale ale modulului antimalware:

1. Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fisierelor putand fi definita de administratorul solutiei,
2. Definirea pana la 16 nivele de profunzime pentru scanarea in arhive.
3. Scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul caruia sunt rulate aplicatii cu potential periculos protejand sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca.
4. Scanarea oricarui suport de stocare a informatiei (CD-uri, harduri externe, unitati partajate etc). De asemenea, se va putea anula scanarea in cazul in care sunt detectate unitati care au informatii stocate mai mult de « x » MB.
5. Scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP.
6. Configurarea cailor ce urmeaza a fi scanate la cerere.
7. Clientii antimalware pentru workstation sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese.
8. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware.
9. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa
10. Produsul antimalware poate fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala. Pentru statiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalata in retea.
11. Pentru o protectie sporita, solutia antimalware trebuie sa aiba 3 tipuri de detectie: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor.
12. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP.
13. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare.
14. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing care va avea si optiunea de verificarea a link-urilor rezultate la cautarea realizata cu motoarele de cautare.

5. Firewall:

1. Posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate.
2. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
3. Posibilitatea de a defini retele de incredere pentru masina destinatie.

6. Carantina:

1. Produsul antimalware sa permita trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului.
2. Trimiterea continutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator.
3. Produsul antimalware sa permita stergerea automata a fisierelor carantinate mai vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare.
4. Posibilitatea de a restaura un fisier din carantina in locatia lui originala.
5. Modulul de carantina va permite rescanarea obiectelor dupa fiecare actualizare de semnaturi.

7. Protectia datelor:

1. Produsul permite blocarea datelor confidentiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

8. Controlul continutului:

1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati:
   a. Permite blocarea accesului la Internet pentru anumite masini client sau grupuri de masini.
   b. Permite blocarea accesului la Internet pe intervale orare.
   c. Permite blocarea paginilor de internet care contin anumite cuvinte cheie.
   d. Permite controlul accesului numai la anumite pagini de internet specificate de administrator;
   e. Permite blocarea accesului la anumite aplicatii definite de administrator;
   f. Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

9. Controlul dispozitivelor:

1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
2. Modulul va permite controlul urmatoarelor tipuri de dispozitive:
   a. Bluetooth Devices
   b. CDROM Devices

c. Floppy Disk Drives
d. Security Policies 153
e. IEEE 1284.4
f. IEEE 1394
g. Imaging Devices
h. Modems
i. Tape Drives
j. Windows Portable
k. COM/LPT Ports
l. SCSI Raid
m. Printers
n. Network Adapters
o. Wireless Network Adapters
p. Internal and External Storage

3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client.
4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

10. Power User:

1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.
2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa si modifica setarile clientului antimalware dintr-o consola dispobibila local pe masina client.
3. Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User.

11. Actualizare:

1. Posibilitatea efectuarii actualizarii la nivel de statie in mod silentios (fara avertizare).
2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
3. Actualizarea pentru locatiile remote prin intermediul unui client antimalware care are si rol de server de actualizare.

D. PROTECTIE SI SECURITATE PENTRU TELEFOANELE MOBILE DE TIP SMARTPHONE

1. Cerinte minime de sistem:

- Telefoane cu sistem de operare iOS 5+: Apple iPhone si tablete iPad
- Telefoane cu sistem de operare Android 2.2+

2. Caracteristici:

1. Permite asocierea unui dispozitiv cu un utilizator din Active Directory.
2. Instalarea se face prin trimiterea unui email catre utilizator cu detaliile de instalare.
3. Activarea dispozitivului mobil in consola de management sa se faca prin scanarea unui cod QR.
4. Pachetele de instalare se vor putea descarca de pe Apple App Store si Google Play.
5. Se vor putea intreprinde urmatoarele actiuni:
    a. Blocarea dispozitivului;
    b. Deblocarea dispozitivului;
    c. Stergerea datelor si revenirea la setarile din fabrica;
    d. Localizarea dispozitivului;
    e. Scanarea dispozitivului(doar pentru cele cu sistem de operare Android);
    f. Criptarea memoriei dispozitivului(doar pentru cele cu sistem de operare Android).
6. Consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel incat utilizatorul sa aiba acces total asupra lui (rooted or jailbroken devices).

3. Setari de securitate:

1. In cazul in care un dispozitiv nu este conform cu setarile dorite, se vor putea intreprinde automat actiunile:
    a. Ignorare;
    b. Blocarea accesului;
    c. Blocarea dispozitivului;
    d. Stergerea datelor si revenirea la setarile din fabrica;
    e. Stergerea dispozitivului din consola.
2. Se va putea impune blocarea dispozitivelor cu ajutorul unei parole. Aceasta parola va putea fi configurata sa contina:
    a. Parola simpla sau complexa (in functie de cerintele sistemului de operare);
    b. Numere si litere;
    c. O lungime minima definita de administrator;
    d. Un numar minim de caractere speciale, definit de adiministrator;

e. Perioada de expirare a parolei. Perioada va putea fi definita de adiministrator;
f. Configurarea restrictiei refolosirii parolei;
g. Numarul de introduceri incorecte a parolei, de catre utilizator;
h. Perioada de autoblocare a dispozitivului dupa un numar de minute definite de adiministrator.

3. Se vor putea genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar si unele legate de accesul la anumite pagini de internet.
4. Profilurile de Wi-Fi vor contine urmatoarele optiuni:
   a. Generale – se defineste SSID precum si tipul securitatii retelei;
   b. Setari TCP/IP – atat pentru protocolul IPv4 dar si pentru IPv6;
   c. Setari de proxy – dezactivat, automat sau configurat manual.
5. Profilurile acces pagini de internet pentru sistemul de operare Android includ optiuni precum:
   a. Permiterea, blocarea sau programarea pentru anumite zile si intervale orare a accesului la anumite pagini de internet;
   b. Crearea unor exceptii pentru blocarea sau permiterea accesului catre anumite pagini de internet.
6. Profilurile acces pagini de internet pentru sistemul de operare iOS inlcud optiuni de activare sau dezactivare a:
   a. Utilizarii browser-ului Safari;
   b. Optiunii de completare automata a informatiilor;
   c. Alertarii utilizatorului in cazul accesarii unor pagini frauduloase;
   d. Javascript;
   e. Pop-up-urilor;
   f. Cookie-uri.

E. PROTECTIE SI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE

1. Produsul va oferi protectie antimalware, antispam (inclusiv antiphishing), precum si filtrare de atasamente si continut, prin integrarea cu serverul Microsoft Exchange. De asemenea, va permite scanarea antimalware la cerere a bazelor de date Exchange.
2. Produsul va asigura scanarea atasamentelor si a continutului mesajelor in timp real, fara a afecta vizibil performanta serverului de mail.

Formularul ofertei (F3.1)

Data depunerii ofertei: **19 Iulie 2017**

Licitaţia Nr.: 17/02303

Invitaţie la licitaţia Nr.: 55 din 11.07.2017

Alternativa Nr.: _____

Către: CASA NAȚIONALĂ DE ASIGURĂRI SOCIALE

SC "RETELE TERESTRE" S.R.L.declară că:

a) Au fost examinate şi nu există rezervări faţă de documentele de atribuire, inclusiv modificările nr *Nu au fost inregistrate modificari.*

b) SC "RETELE TERESTRE" S.R.L. se angajează să furnizeze/presteze, în conformitate cu documentele de atribuire şi condiţiile stipulate în specificaţiile tehnice şi preț, următoarele bunuri şi/sau servicii

- *Soluţia IT antivirală în formă de o platformă integrată de administrare a securităţii, proiectată ca o soluţie modulară*

c) [redacted]

d) [redacted]

e) Prezenta ofertă va rămîne valabilă pentru perioada de timp specificată în **FDA4.8.**, începînd cu data-limită pentru depunerea ofertei, în conformitate cu **FDA5.2.**, va rămîne obligatorie şi va putea fi acceptată în orice moment pînă la expirarea acestei perioade;
În cazul acceptării prezentei oferte, SC "RETELE TERESTRE" S.R.L.se angajează să obţină o Garanţie de bună execuţie în conformitate cu **FDA7**, pentru executarea corespunzătoare a contractului de achiziţie publică.

f) Nu sîntem în nici un conflict de interese, în conformitate cu punctul **IPO5.4**.

g) Compania semnatară, afiliaţii sau sucursalele sale, inclusiv fiecare partener sau subcontractor ce fac parte din contract, nu au fost declarate neeligibile în baza prevederilor legislaţiei în vigoare sau a regulamentelor cu incidenţă în domeniul achiziţiilor publice, în conformitate cu punctul **IPO5.5**.

Semnat: L.Ş.

Nume:Victor CIOCLEA
În calitate de: Administrator
Ofertantul: SC "RETELE TERESTRE" S.R.L.
Adresa: Republica Moldova, mun. Chisinau, str. Mitropolit G. Banulescu-Bodoni 45, of. 415.
Data: 19 Iulie 2017

3. Actualizarea antimalware trebuie sa poata fi facuta automat la un interval de maxim 1 ora, precum si la cerere.
4. In afara de detectia pe baza de semnaturi, modulul de protectie antimalware va trebui sa includa si scanare euristica comportamentala, prin simularea unui calculator virtual in interiorul caruia sunt rulate si analizate aplicatii cu potential periculos, pentru a proteja sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca.
5. Produsul va oferi optiuni multiple de actiune la identificarea unui atasament virusat (dezinfectare, stergere, mutare in carantina).
6. Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va oferi protectie anti-spyware pentru a preveni furtul de date confidentiale.
7. Produsul va oferi protectie antispam, cu o baza de semnaturi actualizabila prin internet.
8. Modulul antispam va trebui sa includa un filtru URL cu o baza de adrese URL cunoscute a fi folosite in mesaje spam, precum si un filtru de caractere pentru detectarea automata a mesajelor scrise cu caractere chirilice sau asiatice.
9. Produsul va trebui sa ofere filtru RBL care sa identifice spam-ul prin sincronizarea cu anumite baze de date online care contin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje.
10. Produsul va trebui sa ofere un serviciu/filtru online pentru imbunatatirea protectiei impotriva valurilor de spam nou aparute.
11. Produsul va oferi posibilitatea de a defini politici de filtrare antimalware, antispam, a continutului sau atasamentelor pentru diferite grupuri sau utilizatori.
12. Actualizarea produsului va fi configurabila si se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul retelei de pe un server de actualizare propriu.
13. Produsul va trebui sa ofere statistici atat referitoare la scanarea antivirus cat si la scanarea antispam.
14. Produsul se va integra in cadrul consolei de management unitar al solutiei antivirus. Pentru usurinta accesului la setarile produsului din diferite medii de operare, produsul va avea consola de administrare web.

F. Alte Cerințe:

15. Producătorul trebuie să ofere suport tehnic, inclusiv in limba romana, prin e-mail sau conectare de la distanță în timpul orelor de lucru din Republica Moldova.
16. Autorizarea de la Producator vis-a-vis de dreptul de vanzare a produselor pe teritoriul R. Moldova;
17. Prezentarea a minim 2 certificate tehnice pe solutia propusa.
18. Disponibilitatea interfeței administratorului în limba română și engleză
19. Support 24/24 în limba Română din partea producătorului si suport local din partea partenerului;

J. Instalare, configurare și training:

1. CERINȚE FAȚĂ DE INSTRUIRE (TRAINING)

	1. Serviciile de instruire (training)
a.	În cadrul proiectului, Vînzătorul va organiza sesiuni de instruire și transfer de cunoștințe pentru salariații Cumpărătorului în vederea formării setului de cunoștințe necesar pentru a permite echipei instruite să preia menținerea și configurarea ulterioară a soluției, în conformitate cu necesitățile **Serviciului Stare Civila**
b.	Instruirea se va organiza pentru diferite grupuri țintă la sediul Cumpărătorului. Grupul tinta: - Analisti - 2 persoane - Administratori ai aplicatiei - 4 persoane, În acest sens, ca parte a ofertei, Ofertantul va prezenta ca parte a ofertei, un plan de instruire, în care se va indica ce tipuri de instruiri va efectua Ofertantul, pentru ce categorie de utilizatori, precum și cuprinsul/agenda acestor instruiri.
c	În afara instruirilor ce țin de utilizarea soluției, Ofertantul trebuie să efectueze și sesiuni de instruire pentru echipa de menținere din partea Cumpărătorului, în scopul asigurării unui nivel adecvat de cunoștințe și competențe, pentru a putea utiliza eficient instrumentele de configurare și dezvoltare disponibile în cadrul soluției.
d	În cadrul serviciilor de implementare, pentru a asigura transferul necesar de cunoștințe către echipa Cumpărătorului, Ofertantul va fi de acord ca cel puțin o persoană să asiste la lucrările de parametrizare/configurare, stabilite de comun acord de către Părți.

e	Ofertantul selectat la etapa de încheiere a contractului, va trebui să elaboreze şi să convină cu Cumpărătorul următoarele elemente ale componentei de instruire: - Strategia Ofertantului cu privire la instruire şi programul de formare; - Structura şi componenţa pachetului de cursuri pentru formare şi a manualelor de studiu pentru fiecare categorie de utilizator; - Metodologia şi procedurile de evaluare şi control al eficienţei şi suficienţei sesiunilor de instruire.
f.	În cadrul sesiunilor de instruire, Ofertantul va pune la dispoziția Cumpărătorului întreg setul de documentație al soluției, care să cuprindă cel puțin următoarele componente: - Ghidurile administratorilor - Ghidurile de instalare și configurare Fișierele surse pentru toate configurările și customizările realizate pe parcursul proiectului

2. CERINȚE FAȚĂ DE SERVICIILE DE IMPLEMENTARE SI CONFIGURARE

Serviciului Stare Civila optează pentru o implementare etapizată a produsului achiziționat.

	Ofertantul selectat va livra licențele pentru soluție, iar **Serviciul Stare Civila** va încheia acordul de licențiere prevăzut în acest scop de către Producătorul licențelor.
	Ofertantul selectat va efectua pregătirea mediului de instalare pentru soluția propusă, după care va asigura implementarea inițială a soluției aplicative în mediul de producție și mediul de testare al (clientului).
c	Ofertantul selectat va efectua configurarea inițială a soluției, atât pentru mediul de producție, cât și mediul de testare. Prin configurare inițială, (Furnizorul) înțelege setarea tuturor paramentrilor aplicabili în corespundere cu cerintele (clientului), inclusiv configurarea și instalarea solutiei ofertate, setarea politicilor și testarea inainte de a fi pusa in productie.
d	În baza rezultatelor de la etapa de design, Ofertantul selectat va implementa toate configurările / customizările agreate darea in exploatare a solutiei.
e	Ofertantul va asigura integrarea soluției cu cel puțin următoarele aplicații terțe:

	- Integrarea cu Active Directory – pentru a asigura autentificarea utilizatorilor în cadrul soluției prin AD; Serviciul de mesagerie electronică (Exchange) – pentru securizarea casutelor postale si activarea antispamului conform cerintelor (clientului). - Integrarea cu platforma mobila (telefoane, tablete) – pentru securizarea perimetrului mobile.
f.	La sfârșitul etapei, Ofertantul va face o demonstrație a soluției și a modulelor care au fost acoperite, fapt care va servi drept unul din criteriile de acceptanță ale etapei de implimentare.
	După acceptanța finală a soluției, va fi activată în mod automat opțiunea de garanție post-implementare si suport. Perioada de garanție post-implementare si suport va fi de 3 ani calendaristici de la data activării acestei opțiuni. Serviciile de garanție post-implementare si suport se referă la serviciile oferite de către Ofertantul selectat adițional la serviciile de mentenanță și suport a licențelor, oferite direct de către producătorul licențelor.
C	Serviciile de garanție post-implementare si suport, vor include următoarele componente: - Gestionarea incidentelor de securitate aparute pe perioada suportului activ; - Solicitărilor de schimbare a politicilor de securiate - Solicitari de analiza si corectie a politicilor de securitate in cadrul companiei implimentate;

Vînzătorul:

SC „Rețele Terestre" S.R.L.

Director

Victor CIOCLEA_____

Cumpărătorul:

Serviciul Stare Civilă

Director adjunct

Veronica BUSUIOC-VOLOSATÎI_____

CONDIŢII SPECIALE

1. Obiectul Contractului

1.1. Vînzătorul îşi asumă obligaţia de a livra produsul software Antivirus conform Specificaţiei (anexa nr. 1 şi anexa nr. 2), care este parte integrantă a prezentului Contract.

1.2. Cumpărătorul se obligă, la rîndul său, să achite şi să recepţioneze Bunurile livrate de Vînzător.

1.3. Calitatea Bunurilor se atestă prin certificatele de calitate prezentate la livrarea Bunurilor. Bunurile livrate în baza contractului vor respecta standardele indicate în Specificaţie. Cînd nu este menţionat nici un standard sau reglementare aplicabilă, se vor respecta standardele sau alte reglementări autorizate în ţara de origine a produselor.

2.Termenele şi condiţiile de livrare

2.1. Produsul software va fi livrat de către Vînzător la sediul Cumpărătorului (str. Mihai Viteazul nr. 11/1, mun. Chişinău) la cererea în scris a acestuia, în termen de 10 zile, ulterior înregistrării corespunzătoare a contractului la Trezoreria de Stat.

2.2. Documentaţia de însoţire a Bunurilor include:

1) originalele facturilor fiscale

2) actul de predare-primire a bunurilor.

2.3. Data livrării Bunurilor se consideră data perfectării facturii fiscale şi recepţionării lor de către Cumpărător.

3. Preţul Contractului şi condiţiile de plată

3.1. Preţul Bunurilor livrate conform prezentului Contract este stabilit în lei moldoveneşti, fiind indicat în Specificaţia prezentului Contract.

3.2. Suma totală a prezentului Contract, inclusiv TVA, se stabileşte în lei moldoveneşti şi constituie: **397200,00 (trei sute nouăzeci şi şapte mii două sute lei, 00 bani) lei** MD.

3.3. Achitarea plăţilor pentru Bunurile livrate se va efectua în lei moldoveneşti.

3.4. Plăţile se vor efectua prin transfer bancar pe contul de decontare al Vînzătorului indicat în prezentul Contract în termen de 14 zile din momentul prezentării facturii fiscale şi a actului de predare-primire a bunului.

4. Condiţiile de predare-primire

4.1. Bunurile se consideră predate de către Vînzător şi recepţionate de către Cumpărător dacă:

a) cantitatea Bunurilor corespunde informaţiei indicate în Specificaţie şi documentele de însoţire conform punctului 2.2 al prezentului Contract;

b) calitatea Bunurilor corespunde informaţiei indicate în Specificaţie;

c) ambalajul şi integritatea Bunurilor corespunde informaţiei indicate în Specificaţie.

4.2. Vînzătorul este obligat să prezinte Cumpărătorului un exemplar original al facturii fiscale odată cu livrarea Bunurilor, pentru efectuarea plăţii. Pentru nerespectarea de către Vînzător a prezentei clauze, Cumpărătorul îşi rezervă dreptul de a majora termenul de achitare prevăzut în punctul 3.4 corespunzător numărului de zile de întîrziere şi de a fi exonerat de achitarea penalităţii stabilite în punctul 9.9.

5. Standarde

5.1 Produsele livrate în baza contractului vor respecta standardele prezentate de către Vînzător în propunerea sa tehnică.

5.2 Cînd nu este menţionat nici un standard sau reglementare aplicabilă se vor respecta standardele sau alte reglementări autorizate în ţara de origine a produselor.

6.Drepturile şi obligaţiile părţilor

6.1. În baza prezentului Contract, ***Vînzătorul*** se obligă:

a) să livreze Bunurile în condiţiile prevăzute de prezentul Contract;

b) să anunţe Cumpărătorul după semnarea prezentului Contract, în decurs de 5 zile calendaristice, prin telefon/fax sau telegramă autorizată, despre disponibilitatea livrării Bunurilor;

c) să asigure condiţiile corespunzătoare pentru recepţionarea Bunurilor de către Cumpărător, în termenele stabilite, în corespundere cu cerinţele prezentului Contract;

d) să asigure integritatea şi calitatea Bunurilor pe toată perioada de pînă la recepţionarea lor de către Cumpărător.

6.2. În baza prezentului Contract, ***Cumpărătorul*** se obligă:

a) să întreprindă toate măsurile necesare pentru asigurarea recepţionării în termenul stabilit a Bunurilor livrate în corespundere cu cerinţele prezentului Contract;

b) să asigure achitarea Bunurilor livrate, respectînd modalităţile şi termenele indicate în prezentul Contract.

7. Forţa majoră

7.1. Părţile sînt exonerate de răspundere pentru neîndeplinirea parţială sau integrală a obligaţiilor conform prezentului Contract, dacă aceasta este cauzată de producerea unor cazuri de forţă majoră (războaie, calamităţi naturale: incendii, inundaţii, cutremure de pămînt, precum şi alte circumstanţe care nu depind de voinţa Părţilor).

7.2. Partea care invocă clauza de forţă majoră este obligată să informeze imediat (dar nu mai tîrziu de 10 zile) cealaltă Parte despre survenirea circumstanţelor de forţă majoră.

7.3 Survenirea circumstanţelor de forţă majoră, momentul declanşării şi termenul de acţiune trebuie să fie confirmate printr-un certificat, eliberat în mod corespunzător de către organul competent din ţara Părţii care invocă asemenea circumstanţe.

8. Rezilierea Contractului

8.1. Rezilierea Contractului se poate realiza cu acordul comun al Părţilor.

8.2. Contractul poate fi reziliat în mod unilateral de către:

a) Cumpărător în caz de refuz al Vînzătorului de a livra Bunurile prevăzute în prezentul Contract;

b) Cumpărător în caz de nerespectare de către Vînzător a termenelor de livrare stabilite;

c) Vînzător în caz de nerespectare de către Cumpărător a termenelor de plată a Bunurilor;

d) Vînzător sau Cumpărător în caz de nesatisfacere de către una dintre Părţi a pretenţiilor înaintate conform prezentului Contract.

8.3. Partea iniţiatoare a rezilierii Contractului este obligată să comunice în termen de 5 zile lucrătoare celeilalte Părţi despre intenţiile ei printr-o scrisoare motivată.

8.4. Partea înştiinţată este obligată să răspundă în decurs de 5 zile lucrătoare de la primirea notificării.

9. Reclamaţii şi sancţiuni

9.1. Reclamaţiile privind cantitatea Bunurilor livrate sînt înaintate Vînzătorului la momentul recepţionării lor, fiind confirmate printr-un act întocmit în comun cu reprezentantul Vînzătorului.
9.2. Pretenţiile privind calitatea Bunurilor livrate sînt înaintate Vînzătorului în termen de 5 zile lucrătoare de la depistarea deficienţelor de calitate şi trebuie confirmate printr-un certificat eliberat de o organizaţie independentă neutră şi autorizată în acest sens.
9.3. Vînzătorul este obligat să examineze pretenţiile înaintate în termen de 5 zile lucrătoare de la data primirii acestora şi să comunice Cumpărătorului despre decizia luată.
9.4. În caz de recunoaştere a pretenţiilor, Vînzătorul este obligat, în termen de 5 zile, să livreze suplimentar Cumpărătorului bunurile nelivrate, iar în caz de constatare a calităţii necorespunzătoare – să le substituie sau să le corecteze în conformitate cu cerinţele Contractului.
9.5. Vînzătorul poartă răspundere pentru calitatea bunurilor în limitele stabilite, inclusiv pentru viciile ascunse.
9.6. În cazul devierii de la calitatea confirmată prin certificatul de calitate întocmit de organizaţia independentă neutră sau autorizată în acest sens, cheltuielile pentru staţionare sau întîrziere sînt suportate de partea vinovată.
9.7. Pentru refuzul de a livra Bunurile prevăzute în prezentul Contract, Vînzătorul suportă o penalitate în valoare de 5 % din suma totală a contractului.
9.8. Pentru livrarea cu întîrziere a Bunurilor, Vînzătorul poartă răspundere materială în valoare de 0,1% din suma Bunurilor livrate, pentru fiecare zi de întîrziere, dar nu mai mult de 5 % din suma totală a prezentului Contract.
9.9. Pentru achitarea cu întîrziere a mărfii, Cumpărătorul poartă răspundere materială în valoare de 0.1% din suma mărfii neachitate, pentru fiecare zi întîrziată, dar nu mai mult de 5 % din suma totală a prezentului contract.

10. Drepturi de proprietate intelectuală

10.1. Vînzătorul are obligaţia să despăgubească Cumpărătorul împotriva oricăror:
a) reclamaţii şi acţiuni în justiţie, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), legate de echipamentele, materialele, instalaţiile sau utilajele folosite pentru sau în legătură cu produsele achiziţionate, şi
b) daune-interese, costuri, taxe şi cheltuieli de orice natură, aferente, cu excepţia situaţiei în care o astfel de încălcare rezultă din respectarea Caietului de sarcini întocmit de către achizitor.

11. Dispoziţii finale

11.1. Litigiile ce ar putea rezulta din prezentul Contract vor fi soluţionate de către Părţi pe cale amiabilă. În caz contrar, ele vor fi transmise spre examinare în instanţa de judecată competentă conform legislaţiei Republicii Moldova.
11.2. De la data semnării prezentului Contract, toate negocierile purtate şi documentele perfectate anterior îşi pierd valabilitatea.
11.3 Părţile contractante au dreptul, pe durata îndeplinirii contractului, să convină asupra modificării clauzelor contractului, prin act adiţional, numai în cazul apariţiei unor circumstanţe care lezează interesele comerciale legitime ale acestora şi care nu au putut fi prevăzute la data încheierii contractului. Modificările şi completările la prezentul Contract sînt valabile numai în cazul în care au fost perfectate în scris şi au fost semnate de ambele Părţi.
11.4. Nici una dintre Părţi nu are dreptul să transmită obligaţiile şi drepturile sale stipulate în prezentul Contract unor terţe persoane fără acordul în scris al celeilalte părţi.
11.5. Prezentul Contract este întocmit în 2 exemplare în limba de stat a Republicii Moldova, cîte un exemplar pentru Vînzător şi Cumpărător.
11.6. Prezentul Contract se consideră încheiat la data semnării şi intră în vigoare după înregistrarea lui de către Trezoreria de Stat, fiind valabil pînă la *31 decembrie 2016*.