ANUNȚ/INVITAȚIE DE PARTICIPARE
(Formatul documentului nu va fi modificat)

1. **Denumirea autorității contractante:** Agenția de Transplant
2. **IDNO:** 1010601000139
3. **Tipul procedurii de achiziție:** achiziții de bunuri
4. **Obiectul achiziției:** Procurarea programului antivirus (Pachetul software antivirus).
   Cod CPV – 48761000 - 0

Prezentul anunț de participare este întocmit în scopul achiziționării:

5. Procurarea programului antivirus (Pachetul software antivirus).

(obiectul achiziției)

conform necesităților Agenției de Transplant
(denumirea autorității contractante)

(în continuare – Cumpărător) pentru perioada bugetară 2018, este alocată suma necesară din: Trezoreria Regională Chișinău Bugetul de Stat
(sursa banilor publici)

Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind **livrarea**/prestarea/executarea următoarelor **bunuri** /servicii/lucrări:

Nr. d/o	Cod CPV	Denumirea bunurilor solicitate	Unit. de măsură	Cantitatea	Specificarea tehnică deplină solicitată, standarde de referință
1.	48761000-0	Procurarea programului antivirus (Pachetul software antivirus pentru 12 computatoare + server)	Lot	1	Vezi anexa nr. 1
		TOTAL	**LOT**		**Preț fără TVA/Preț cu TVA**

6. **Termenul de livrare/prestare/executare solicitat și locul destinației finale:**
31 decembrie 2019, str. Testemițanu, 29, mun. Chișinău

7. **Tipul contractului:** de livrare a bunurilor.

8. **Termenul și condițiile de executare solicitat (durata contractului):** de la data înregistrării contractului la Trezoreria Regională Chișinău Bugetul de Stat

9. **Termenul de valabilitate a contractului (luni):** 31.12.2019

10. **Modalitatea de efectuare a evaluării:** **Un singur lot**

Documentele/cerinţele de calificare pentru operatorii economici includ următoarele:

Nr. d/o	Denumirea documentului/cerinţei	Cerinţe suplimentare faţă de document	Obligativitatea
1.	**Oferta**	Original: confirmată prin semnătura şi ştampila umedă a operatorului economic.	**Da**
2.	**DUAE**	Original: confirmată prin semnătura şi ştampila umedă a operatorului economic.	**Da**

Operatorii economici interesaţi pot obţine informaţie suplimentară sau pot solicita clarificări de la autoritatea contractantă la adresa indicată mai jos:
Denumirea autorităţii contractante: Agenţia de Transplant
Adresa: mun. Chişinău, str. Testemiţanu, 29
Tel: 069167204
Fax: 022 28-64-61
E-mail: iamandi.liliana@yahoo.com
Numele şi funcţia persoanei responsabile: Iamandii Liliana, jurist
Întocmirea ofertelor: ***Oferta şi documentele de calificare solicitate*** vor fi întocmite clar, fără corectări, cu număr şi dată de ieşire, cu semnătura persoanei responsabile.
Criteriul de atribuire este: *cel mai mic preţ fără TVA şi corespunderea cerinţelor din specificaţia tehnică.*

Termenul de valabilitate a ofertelor: *30 zile calindaristice, de la data depunerii ofertei.*
Valoarea estimativă a achiziţiei, fără TVA, lei: 10 600,00.

Preşedintele grupului de lucru: _____ **Igor CODREANU**

Anexa nr. 1

SPECIFICAȚIA TEHNICĂ

Nr. crt	Denumirea bunurilor	Cod CPV	Cantitatea (bucăți)	Prețul MD (incl. TVA)	Suma totală MD (inclusiv TVA)
1.	Procurarea programului antivirus (Pachetul software antivirus pentru 12 computatoare + server), **vezi anexa nr. 2**	48761000 - 0	12 + server = 13		
	TOTAL				

Anexa nr. 2

I. Componente ale sistemului antivirus:

A. Protecţie

1. Controlul programelor active

* Încredere faţa de programele care au o semnătură digitală

Pentru programe necunoscute:

* Introducerea automată într-un grup (restricţii slabe, restricţii puternice, nesigur)
* Utilizare analiza euristică pentru a determina grupul
* Eliminare regulile de control ale programului care nu au accesate mai mult de un anumit număr de zile.

2. File Anti –Virus

* Nivel de securitate (scăzut, recomandat, ridicat)
* Acţiune când se detectează o ameninţare (solicitaţi acţiune, blocaţi accesul (dezinfectaţi / ştergeţi dacă dezinfecţia nu reuşeşte))
* Tipuri de fişiere (toate fişierele, fişierele scanate după format, fişierele scanate prin extensie)
* Localizare (toate unităţile detaşabile, toate unităţile hard disk, toate unităţile de reţea)
* Analiza semnăturii
* Analiza euristică (suprafaţă, medie, profundă)
* Optimizărea verificării
  - Scanarea numai a fişierelor noi şi modificate
* Verificarea fişierelor compuse:
  - Scanare arhive
  - Verificare pachetele de instalare
  - Verificare obiecte OLE imbricate
  - Verificare obişnuită - opţională (despachetaţi fişierele compuse în fundal / despachetaţi fişiere compozite de dimensiuni mari)
* Modul de testare (inteligent, la accesarea şi schimbarea, la accesare, în timpul execuţiei)
* Tehnologii de scanare (iSwift, iChecker)
* Suspendarea sarcinii (conform programului, la începutul programelor) este opţională

3. Firewall

* Reguli pentru programe
* Reguli pentru pachete
* Zone (reţele disponibile)
* Sistem de detectare a intruziunilor

-blocaţi computerul atacat pentru un anumit număr de minute

4. Antivirusul poştal

* Nivel de securitate (scăzut, recomandat, ridicat)
* Zonă de protecţie (numai mesaje primite şi trimise / mesaje primite)
* Integrarea în sistem (POP3 trafic / SMTP / NNTP / IMAP, ICQ / MSN, MS Office Outlook plug-in, plug-in The Bat)
* Metodele de verificare (a verifica link-urile pe baza Web-link-uri suspecte, verificare link-urile pe baza fishingWeb-link-uri)
* Analiza euristică (suprafaţă, medie, profundă)
* Verificarea fişierelor compuse:
  - Posibilitatea de scanaţi ori ne scanare arhivele
  - Posibilitatea de scanaţi ori ne scanare obiecte cu un anumit volum
* Filtru ataşament (după formatul fişierului)

5.Web-antivirus

* Metode de verificare (verificaţi linkurile către baza de date a adreselor Web suspecte, verificaţi linkurile către baza de date a adreselor Web de fishing)

* Limitaţi timpul cache al fragmentelor în câteva secunde.
* adrese de încredere (add / change / delete / export / import)
* Acţiune (cerere / bloc / permite)

6. Protecţie proactivă
* Analiza activităţii proceselor
* Monitorizarea sistemului de registru

7. Anti-hacker
* Reguli pentru programe
* Reguli pentru pachete
* Zone (reţele disponibile)
* Sistem de detectare aintruziunilor
  · Blocaţi computerul atacat pentru un anumit număr de mine.

8. Anti-Spy
* Anti-banner (listaneagră, listaalbă)
* Anti-apelare (adrese de încredere)

9. Anti-Spam
* Nivelul de agresivitate (scăzut, recomandat, ridicat, blocaţi tot)
* Integrarea în sistem (POP3 trafic / SMTP / NNTP / IMAP, ICQ / MSN, MS Office Outlook plug-in, plug-in The Bat)
* Metodele de verificare (a verifica link-urilepebaza Web-link-urisuspecte, verificaţi link-urilepebaza phishing Web-link-uri)
* Algoritmi pentru recunoaştere (analiza expresii lor pe baza de date Resent Terms, utilizarea unei baze de date extinse, analiza anteturilor şi mesajelor PDB, recunoaştere a imaginii GSG, algoritmul de auto-învăţare Bayes pentru analiza textului)
* Lista albă
* Lista neagră
*Instruire (prezenţa maestrului de formare)

10. Controlul accesului
* Lista dispozitivelor blocate
* Autostart (dezactivaţi autor un pentru toate dispozitivele, dezactivaţi autorun.inf)

II. Scanare
Tipuri:
1. Scanare completă
2. Scanare rapidă

Specificarea:
* Nivel de securitate (scăzut, recomandat, ridicat)
* Acţiune când se detectează o ameninţare (cereţi la sfârşitul scanării, cereţi în timpul scanării, nu întrebaţi: trataţi, ştergeţi dacă tratamentul nu este posibil)
* Modul de lansare (în fiecare zi, în fiecare zi lucrătoare, la fiecare oră, în fiecare zi a lunii)
* Domeniul de aplicare (toate fişierele, fişierele scanate după format, fişierele scanate prin extensie)
* Verificarea fişierelor compuse:
  - Scanare arhive
  - Verificare pachetele de instalare
  -Verificare obiecte OLE imbricate
  - Scanare fişierelor de format e-mail
  - Scanare arhive protejate prin parolă
* Analizae uristică (suprafaţă, medie, profundă)
* Tehnologii de scanare (iSwift, iChecker)
* Căutare Rootkit

* Modul de lansare: executare sarcina cu drepturi de cont (nume de utilizator, parolă)

III. Actualizare

* Mod de pornire: automat, după o anumită perioadă, manual
* Setări proxy
* Actualizare sursă (servere de actualizare firmei- producatorului. Servere de administrare, surse adăugătoare)
* Modul de pornire:
  - executare sarcina cu drepturi de cont (nume de utilizator, parolă)
* Distribuirea actualizărilor:
  -Copiați actualizările într-un dosar (adresa dosarului)

IV. Mai multe opțiuni

* Auto-apărare a programului
* Dezactivare controlul extern al programului
* Protecția prin parolă
* Nu executați sarcini programate atunci când rulează pe baterie
* Carantină și spațiu de stocare de rezervă (nu maimult de un anumit număr de zile de stocare a obiectelor, dimensiunea obiectelor, verificarea fișierelor în carantină după actualizare)
* Posibilitatea de controlate porturi (Control toate porturile / porturile selectate)
* Protecție antivirus pentru nodurile principale ale unei rețele: stații de lucru, laptopuri, servere de fișiere;
* Producătorul trebuie să facă parte din grupul programelor Gartner 2019;
* Produsul trebuie să salveze obiectele identificate ca fiind suspecte în carantină sau într-un director dedicat în format criptat.

* Produsul trebuie să permită ca instalarea să fie efectuată pe un computer local sau la distanță. Produsul trebuie să ofere suport pentru sisteme de operare Windows.

* Consola de administrare a produsului trebuie sa fie instalata on-premis.
* Produsul trebuie să permit instalarea dintr-un singur kit de instalare care să includă toate pachetele necesare pentru implementare.

* Produsul trebuie să ofere administratorului posibilitatea de împiedicare a acțiunilor periculoase pentru sistemul de operare ale aplicațiilor, și să asigure controlul accesului la resursele sistemului de operare și la datele confidențiale.

* Produsul trebuie să permită crearea, păstrarea și implementarea imaginilor a sistemului de operare, cu ajutorul consolei de administrare dedicată.
* Produsul trebuie să permit detectarea automată a vulnerabilităților din sistemul de operare și a aplicațiilor instalate.
* Produsul trebuie să permita administratorului să identifice toate încercările utilizatorului de pornirea aplicației și să reglementeze lansarea aplicațiilor prin intermediul regulilor de control pentru pornirea aplicațiilor.

II. Cerințe față de Furnizorul de program antivirus licențiat:

* Prezentarea de către Prestator a unui document de parteneriat confirmativ și MAF parvenit de la compania producător/filiala companiei producător.
* Furnizorul trebuie sa ofere instruiri gratuite pentru administratori de fiecare data când apare o versiune nou a solutiei.