ANUNȚ DE PARTICIPARE

privind achiziționarea a licenței pentru antivirus pentru anul 2020
prin achiziția de valoare mică

1. **Denumirea autorității contractante:** IMSP Spitalul Clinic Republican „Timofei Moșneaga”
2. **IDNO:** 1003600150783
3. **Adresa:** MD-2025, mun.Chișinău, str.Nicolae Testemițanu 29
4. **Numărul de telefon/fax:** 022 403 697
5. **Adresa de e-mail și de internet a autorității contractante:** www.scr.md/ achizitiipublicescr@gmail.com
6. **Adresa de e-mail sau de internet de la care se va putea obține accesul la documentația de atribuire:** ***documentația de atribuire este anexată în cadrul procedurii în SIA RSAP***
7. **Obiectul achiziției:** Achiziționarea a licenței pentru antivirus pentru anul 2020
8. **Cod CPV:** 48760000-3
9. **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. lot	Cod CPV	Denumirea serviciilor solicitate	U/M	Cantitatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată, fără TVA, lei
1	48760000-3	Licență pentru antivirus pentru anul 2020	buc	100	**I. Componente ale sistemului antivirus:** **A.Potecție** **1.Controlul programelor active** * Încredere fața de programele care au o semnătură digitală Pentru programe necunoscute: * Introducerea automată într-un grup (restricții slabe, restricții 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) * Acțiune când se detectează o amenințare (solicitați acțiune, blocați accesul (dezinfectați / ștergeți dacă dezinfecția nu reușește)) * Tipuri de fișiere (toate fișierele, fișierele scanate după format, fișierele scanate prin extensie) * Localizare (toate unitățile detașabile, toate unitățile hard disk, toate unitățile de rețea) * Analiza semnăturii * Analiza euristică (suprafață, medie, profundă) * Optimizăreaverificării - Scanarea numai a fișierelor noi și modificate * Verificarea fișierelor compuse: - Scanare arhive - Verificare pachetele de instalare -Verificare obiecte OLE imbricate - Verificare obișnuită - opțională (despachetați fișierele compuse în fundal / despachetați fișiere compozite de dimensiuni mari) * Modul de testare (inteligent, la accesarea și schimbarea, la accesare, în timpul execuției) * Tehnologii de scanare (iSwift, iChecker) * Suspendarea sarcinii (conform programului, la începutul programelor) este opțională	

3.Firewall
* Reguli pentru programe
* Reguli pentru pachete
* Zone (rețele disponibile)
* Sistem de detectare a intruziunilor
-blocați computerul atacat pentru un anumit număr de minute

4.Antivirusul postal
* Nivel de securitate (scăzut, recomandat, ridicat)
* Zonă de protecție (numai mesaje primite și 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 (suprafață, medie, profundă)
* Verificarea fișierelor compuse:
- Posibilitatea de scanați ori ne scanare arhivele
- Posibilitatea de scanați ori ne scanare obiecte cu un anumit volum
* Filtru atașament (după formatul fișierului)

5.Web-antivirus * Metode de verificare (verificați linkurile către baza de date a adreselor Web suspecte, verificați linkurile către baza de date a adreselor Web de fishing)
* Limitați timpul cache al fragmentelor în câteva secunde.
* adrese de încredere (add / change / delete / export / import)
* Acțiune (cerere / bloc / permite)

6.Protecție proactivă
* Analiza activității proceselor
* Monitorizarea sistemului de registru

7.Anti-hacker
* Regulipentruprograme
* Regulipentrupachete
* Zone (rețele disponibile)
* Sistem de detectareaintruziunilor
Blocați 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, blocați tot)
* Integrareaînsistem (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, verificați link-urilepebaza phishing Web-link-uri)
* Algoritmipentrurecunoaștere (analiza expresiilorpebaza de date Resent Terms, utilizareauneibaze de date extinse, analiza anteturilormesajelor PDB, recunoaștere a imaginii GSG, algoritmul de auto-învățarei Bayes pentru analiza textului)
* Lista albă
* Lista neagră
*Instruire (prezența maestrului de formare)

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

B. Scanare

1.Scanare completă
2.Scanare rapidă
Specificarea:
* Nivel de securitate (scăzut, recomandat, ridicat)
* Acțiunecând se detectează o amenințare (cereți la sfârșitul scanării, cereți în timpul scanării, nu întrebați: tratați, ștergeți 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 fișierele, fișierele scanate după format, fișierele scanate prin extensie)
* Verificarea fișierelor compuse:
- Scanare arhive
- Verificare pachetele de instalare
-Verificare obiecte OLE imbricate
- Scanare fișierelor de format e-mail
- Scanare arhive protejate prin parolă
* Analizae uristică (suprafață, medie, profundă)
* Tehnologii de scanare (iSwift, iChecker)
* Căutare Rootkit
* Modul de lansare: executare sarcina cu drepturi de cont (nume de utilizator, parolă)

C.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)

D.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 liderilor ori a vizionarilor în ceea ce privește protecția pentru endpoint așa cum este definit de Gartner 2019.
* Produsul trebuie să salveze obiectele identificate ca fiind suspecte în carantină sau într-undirector dedicat în format criptat.
* Produsul trebuie să permită ca instalarea să fie efectuată pe un computer local sau la distanță. Produsul trebuie să efere support pentru sisteme de operare Windows.
* Consola de administrare a produsului trebuie sa fie instalata on-premis (nu se accepta consola web).
* 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 acesului 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 Furnizor a unui document de parteneriat confirmativ si autorizație (MAF) parvenit de la compania producătoare/filiala companiei producătoare (Copia documentelor de parteneriat și de autorizare). *Posesia a cel puțin 2 specialiști certificați de compania producătoare (Copia certificatelor) *Posesia unui centru de suport local (Copia certificatului)	
					III. Condiții suplimentare: *Furnizorul trebuie sa ofere instruiri gratuite pentru administratori de fiecare dată când apare o versiune nouă a soluției. *În cazul unei alte soluții de securitate cu endpoint decât Kaspersky, Furnizorul trebuie să includă în ofertă și instruirea a 4 persoane în privința utilizării și administrării soluției oferite.	
	TOTAL					**45 000,00**

10. În cazul în care contractul este împărțit pe loturi un operator economic poate depune oferta (se va selecta): 1) Pentru un singur lot.

11. Admiterea sau interzicerea ofertelor alternative: nu se admite

12. Termenii și condițiile de livrare/prestare/executare solicitați: la solicitare, în decurs de 10 zile din data comenzii pe parcursul anului 2020;

13. Termenul de valabilitate a contractului: 31 decembrie 2020

14. Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție; nivelul minim (nivelurile minime) al (ale) cerințelor eventual impuse, se menționează informațiile solicitate (DUAE, documentație):

Nr. d/o	Descrierea criteriului/cerinței	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativit.
1	Informații generale despre ofertant	Să conțină obligatoriu numele conducătorului, date de contact (telefon și e-mail) și coordonatele bancare – confirmat prin semnătura electronică;	Obligatoriu
2	Oferta conform modelului atașat	Încărcată la procedură, confirmată prin semnătura electronică;	Obligatoriu
3	Prezentarea de dovezi privind conformitatea produsului identificată prin referire la specificații sau standarde relevante	Copie confirmată prin aplicarea semnăturii electronice;	Obligatoriu
4	Termen de garanție	Declarație pe propria răspundere privind termenul de garanţie a filtrului nu mai mic de 12 luni din data instalării, confirmată prin aplicarea semnăturii electronice;	Obligatoriu
5	Prezentarea de către Furnizor a unui document de parteneriat confirmativ si autorizație (MAF) parvenit de la compania producătoare/filiala companiei producătoare (Copia documentelor de parteneriat și de autorizare).	(Copia documentelor de parteneriat și de autorizare) ;	Obligatoriu
6	Posesia a cel puțin 2 specialiști certificați de compania producătoare (Copia certificatelor)	(Copia certificatelor) ;	Obligatoriu
7	Posesia unui centru de suport local (Copia certificatului)	(Copia certificatelor)	Obligatoriu
Modalitatea de efectuare a evaluării		Cel mai mic preţ fără TVA cu corespunderea cerinţelor solicitate, pe lot;	Obligatoriu

Termenul de livrare/prestare	La solicitare, în decurs de 10 zile din data comenzii pe parcursul anului 2020;	Obligatoriu
Termen și modalitatea de achitare	Prin transfer, în termen de 30 zile, din data prezentării facturii.	Obligatoriu
Notă: În cazul în care documentele ofertelor încărcate nu vor fi semnate cu **semnătura electronică**, acestea vor fi respinse, potrivit cadrului normativ în vigoare.		

.

15. **Tehnici și instrumente specifice de atribuire (dacă este cazul specificați dacă se va utiliza acordul-cadru, sistemul dinamic de achiziție sau licitația electronică):** licitație electronică. Numărul rundelor – 3. Durata rundelor este stabilită de sistem. Pasul minim – 1% din suma totală a lotului fără TVA.
16. **Condiții speciale de care depinde îndeplinirea contractului (**indicați după caz**):** nu se aplică
17. **Criteriul de evaluare aplicat pentru adjudecarea contractului:** Cel mai mic preţ fără TVA cu corespunderea cerinţelor solicitate, pe lot
18. **Termenul limită de depunere/deschidere a ofertelor:**
    - **până la:** ***[ora exactă]*** SIA RSAP
    - **pe:** ***[data]*** SIA RSAP
19. **Adresa la care trebuie transmise ofertele sau cererile de participare:**

    Ofertele sau cererile de participare vor fi depuse electronic prin intermediul SIA RSAP
20. **Locul deschiderii ofertelor:** SIA RSAP
    Ofertele întârziate vor fi respinse.
21. **Limba sau limbile în care trebuie redactate ofertele sau cererile de participare:** româna
22. **Denumirea și adresa organismului competent de soluționare a contestațiilor:**
    Agenția Națională pentru Soluționarea Contestațiilor
    Adresa: mun. Chișinău, bd. Ștefan cel Mare și Sfânt nr.124 (et.4), MD 2001;
    Tel/Fax/email: 022-820 652, 022 820-651, contestatii@ansc.md
23. **Data transmiterii spre publicare a anunțului de participare:** SIA RSAP
24. **În cadrul procedurii de achiziție publică se va utiliza/accepta:**

Denumirea instrumentului electronic	**Se va utiliza/accepta sau nu**
depunerea electronică a ofertelor sau a cererilor de participare	Se acceptă
sistemul de comenzi electronice	Nu se acceptă
facturarea electronică	Se acceptă
plățile electronice	Se acceptă

25. **Alte informații relevante:** nu sunt

Conducătorul grupului de lucru: _____ Grigore Bobeico