ANUNȚ DE PARTICIPARE

privind achiziționarea Licenței antivirus pentru anul 2022
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:** 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. **Tipul autorității contractante și obiectul principal de activitate (dacă este cazul, mențiunea că autoritatea contractantă este o autoritate centrală de achiziție sau că achiziția implică o altă formă de achiziție comună):** instituție medico-sanitară
8. **Procedura a fost inclusă în planul de achiziții publice a autorității contractante (Da/Nu):** Nu, urmează a fi inclusă în planul de achiziții provizoriu 2022 (aprobat de MS)
   Link-ul către planul de achiziții publice publicat: -
9. **Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind livrarea/prestarea/executarea următoarelor servicii:**

Nr. d/o	Cod CPV	Denumirea bunurilor solicitate	U/M	Canti-tatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată, fără TVA, lei
1	48760000-3	**Lot 1. Licență antivirus pentru anul 2022**	Licența anuală	100	**I. Componente ale sistemului antivirus:** A. Protecție 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) * Optimizarea verificării	**37 500,00**

					- 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 - blocarea calculatorului atacat pentru un anumit număr de minute **4. Antivirusul poștal** * 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 fishing Web-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 detectarea intruziunilor 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) * 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-uri suspecte, verificați link-urile pe baza phishing Web-link-uri) * Algoritmi pentru recunoaștere (analiza expresiilor pe baza de date Resent Terms, utilizarea unei baze de date extinse, analiza anteturilor mesajelor PDB, recunoaștere a imaginii GSG, algoritmul de auto-învățarei Bayes pentru analiza textului) * Lista albă * Lista neagră *Instruire (prezența maestrului de formare) **B. Scanare** Tipuri: 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 * Sursa de actualizare (serverele de actualizare ale companiei producătoare, servere de administrare, surse adăugătoare) * Modul de pornire: - executare sarcina cu drepturi de cont (nume de utilizator, parolă) * Distribuirea actualizărilor: -Copierea actualizărilor într-un dosar (cu indicarea de către utilizator a adresei dosarului) **D. Mai multe opțiuni** * Auto-apărarea programului * Dezactivarea controlului extern al programului * Protecția prin parolă * Neexecutarea sarcinilor programate atunci când rulează pe baterie * Carantină și spațiu de stocare de rezervă (nu mai mult 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-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-premise (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 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 permită detectarea automată a vulnerabilităților din sistemul de operare și a aplicațiilor instalate. - Produsul trebuie să permită administratorului să identifice toate încercările utilizatorului de pornire a aplicațiilor 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). - Copia certificatelor a cel puțin 2 specialiști certificați de compania producătoare. - Posesia unui centru de suport local (Copia certificatului). **III. Condiții suplimentare:** - Furnizorul trebuie să ofere instruiri gratuite pentru 4 persoane de fiecare dată când apare o versiune nouă a soluției. În cazul în care în decursul anului nu apare nici una se efectuează cel puțin o instruire gratuită pentru 4 persoane pentru menținerea nivelului de cunoaștere a soluției de securitate cu endpoint date. '- În cazul unei alte soluții de securitate cu endpoint decât Kaspersky, Furnizorul trebuie să efectueze gratuit instruirea a 4 persoane în privința instalării, utilizării și administrării	

					soluției oferite până la 30 decembrie 2021. '- La necesitatea și cererea Beneficiarului, Furnizorul trebuie să efectueze gratuit auditul instalării, setărilor de securitate a soluției cu endpoint oferite și să ofere o listă de recomandări de modificare/adaptare a lor cu scopul minimizării riscurilor de securitate pentru Beneficiar.	
Valoarea estimativă totală						**37 500,00**

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: După încheierea contractului, la solicitare;

13. Termenul de valabilitate a contractului: 31 decembrie 2022;

14. Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție; nivelul minim/obligativitatea cerințelor eventual impuse; se menționează informațiile solicitate:

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 – confirmată prin aplicarea semnăturii electronice;	Obligatoriu
2	Oferta conform modelului atașat	Încărcată la procedură, confirmată prin aplicarea semnăturii electronice;	Obligatoriu
3	Certificat / Decizie/ Extras de înregistrare	Copie, emis de Agenţia Servicii Publice, confirmată prin aplicarea semnăturii electronice;	Obligatoriu
4	Declarații pe propria răspundere	Declarații pe propria răspundere privind: **1.** Termenul de garanție a licenței pentru antivirus pentru calculatoare de 12 luni (01 ianuarie 2022 – 31 decembrie 2022), confirmată prin semnătura electronică; **2**. Furnizorul va instrui gratuit 4 persoane de fiecare dată când apare o versiune nouă a soluției. În cazul în care în decursul anului nu apare nici una, se efectuează cel puțin o instruire gratuită pentru 4 persoane pentru menținerea nivelului de cunoaștere a soluției de securitate cu endpoint date; **3.** În cazul unei alte soluții de securitate cu endpoint decât Kaspersky, Furnizorul trebuie să efectueze gratuit instruirea a 4 persoane în privința instalării, utilizării și administrării soluției oferite până la 30 decembrie 2021; **4.** La necesitatea și cererea Beneficiarului, Furnizorul trebuie să efectueze gratuit auditul instalării, setărilor de securitate a soluției cu endpoint oferite și să ofere o listă de recomandări de modificare/adaptare a lor cu scopul minimizării riscurilor de securitate pentru Beneficiar.	Obligatoriu

5	Prezentarea de către operatorul economic a unui document de parteneriat confirmativ și autorizație (MAF) parvenită de la compania producătoare / filiala companiei producătoare	Copie, documente de parteneriat și de autorizare, confirmată prin semnătura electronică;	Obligatoriu
6	Posesia a cel puțin 2 specialiști certificați de compania producătoare	Copie, certificatele specialiștilor, confirmată prin semnătura electronică;	Obligatoriu
7	Posesia unui centru de suport local	Copie, certificate, confirmată prin semnătura electronică;	Obligatoriu
Modalitatea de efectuare a evaluării		Cel mai mic preţ fără TVA cu corespunderea cerinţelor solicitate, pe lot	
Termenii și condițiile de livrare/prestare/executare solicitați		După încheierea contractului, la solicitare.	
Termen și modalitate de achitare		Prin transfer, în termen de 30 zile, după livrare/prestare, cu prezentarea facturii;	

15. Tehnici și instrumente specifice de atribuire (dacă este cazul specificați dacă se va utiliza acordul-cadru, sistemul dinamic de achiziție sau licitația electronică): nu se aplică.

16. Criteriul de evaluare aplicat pentru adjudecarea contractului: Cel mai mic preţ fără TVA cu corespunderea cerinţelor solicitate, pe lot.

17. Termenul limită de depunere/deschidere a ofertelor:
- **până la:** SIA RSAP
- **pe:** SIA RSAP

18. Adresa la care trebuie transmise ofertele sau cererile de participare:

Ofertele sau cererile de participare vor fi depuse electronic prin intermediul SIA RSAP

19. Locul deschiderii ofertelor: SIA RSAP
Ofertele întârziate vor fi respinse.

20. Limba sau limbile în care trebuie redactate ofertele sau cererile de participare: româna

21. 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

22. Data transmiterii spre publicare a anunțului de participare: SIA RSAP

23. 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	Se acceptă
facturarea electronică	Se acceptă
plățile electronice	Se acceptă

Conducătorul grupului de lucru: _____ Dragoș PIDLEAC