

## ANUNȚ DE PARTICIPARE

privind achiziționarea Server cu instalare și mentenanță și antivirus software  
(se indică obiectul achiziției)  
prin procedura de achiziție cererea ofertelor de prețuri  
cu licitație electronică, pas minim 0,3%, 3 runde  
(tipul procedurii de achiziție)

1. Denumirea autorității contractante: Agenția Națională pentru Siguranța Alimentelor
2. IDNO: 1013601000082
3. Adresa: mun. Chișinău, str. M. Kogălniceanu, 63
4. Numărul de telefon/fax: 022-26-46-48
5. Adresa de e-mail și de internet a autorității contractante: info@ansa.gov.md
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): autoritate publică
8. 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/ serviciilor/ lucrărilor solicitate	Unitate de măsură	Cantitate	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată fără TVA
<b>Lot 1</b>						
1	48820000-2	Server	buc	1	<p><b><u>Cerințe generale:</u></b> Bunurile oferite în cadrul achiziției trebuie să fie noi, calitative, produse de producători renumiți, bine cunoscuți internațional în domeniul TI. Configurația echipamentului trebuie să fie compusă din componente reciproc compatibile și să asigure funcționarea optimă a bunului în ansamblu. Produsul oferit va trebui să poată fi extins prin achiziția ulterioară a unui sistem de tip back-up, replicare și disaster recovery de la același vendor pentru a exista o integrare nativă a soluției. Produsele oferite trebuie să se regăsească în Gartner, cadrulul de lideri.</p> <p><u>Tip:</u> Server de virtualizare pentru aplicații va avea următoarele caracteristici minime: - <u>Chassis:</u> Rack mount 2U, up to 8 x 2.5" SAS/SATA Hard Drives for 1/2CPU Configuration; - <u>Processor:</u> One (1x) 10 Core processor,  equivalent Intel Xeon Silver 4210 2.2G, 10C/20T, 9.6GT/s, 13.75M Cache, Turbo, HT (85W) DDR4-2400; - <u>Riser Config</u> 1, 4 x 8 slots - <u>Memory:</u> 4x16GB RDIMM, 2666MT/s, Dual Rank; - <u>RAID controller:</u> min 2GB NV Cache, cu posibilitatea de extindere pînă la 8GB</p>	250000

- RAID levels 0, 1, 5, 6
- RAID spans 10, 50, 60
- Online Capacity Expansion (OCE)
- Online RAID Level Migration (RLM)
- Auto resume after power loss during array rebuild or reconstruction/RLM
- Consistency Check for background data integrity
- Physical disk power management
- NVRAM "Wipe" feature protects proprietary data once card is decommissioned
- SED drive support
- Load balancing
- Fast initialization for quick array setup
- Configurable stripe size up to 1MB
- Patrol read for media scanning and repair
- DDF compliant
- Configuration on Disk (COD)
- S.M.A.R.T. support
- Global and dedicated hot spare with revertible hot-spare support, automatic rebuild, enclosure affinity, and emergency SATA;
- Hard drives:
  - Four (4x) 4 x 2.4TB 10K RPM SAS 12Gbps 512e 2.5in Hot-plug Hard Drive,
- Cooling system: High performance fan;
- Power supply: Dual, Hot-plug, Redundant Power Supply (1+1), max 750W;
- Network interfaces:
  - Four (4x) - 1 Gbit Ethernet NIC ports;
  - Two (2x) - 10 Gbit SFP+ NIC ports;
- Ports:
  - Front ports: 1xVGA, 2 x USB 2.0, 1x USB 3.0, dedicated management port
  - Rear ports: 1xVGA, 1x Serial, 2 x USB 3.0, dedicated management network port
- Diagnostic LEDs: On front panel, the ability to install the front panel with WiFi and Bluetooth module for connecting and diagnosing from mobile devices;
- Server management (SM):
  - Must deliver advanced, agent-free local and remote server administration;
  - Local and remote control of system resources (manage, diagnose and monitor);
  - Remote power control, remote firmware updating, remote presence;
  - Support management interfaces IPMI2.0, WEB, WSMAN, SNMP, SSH;
  - LDAP user authentication, Active Directory;
  - "ZeroTouch deployment and provisioning" automated deployment;
  - Support protocols IPv4, IPv6, DNS, DDNS, DHCP;
  - Support of Single Sign-on and 2FA;
  - Notifications for alerts SNMP, Email, IPMI.
  - Browser based administration with, full control over the remote host server's display; keyboard, and mouse, including host OS graphical interface;
  - Virtual media option that provides virtual CD

				<p>drive and remote image mounting;</p> <ul style="list-style-type: none"> <li>• SM &amp; server diagnostics logging;</li> </ul> <p>- <u>Rack mounting rails</u>: ReadyRails Sliding Rails with Cable Management Arm;</p> <p>- <u>Operating Systems Supported</u>: Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server with Hyper-V, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi.</p> <p>- <u>Certificates</u>: EU Declaration of Conformity, Regulatory and Environmental compliance;</p> <p>- <u>Power Efficiency</u>: Energy Star certified;</p> <p><i>Notă:</i> Pentru administratorul IT din cadrul instituției se va organiza instruire de exploatare eficientă a sistemului.</p> <p>Existenta accesului la un Centru de Deservire tehnica pentru deservirea echipamentului propus.</p>		
	<b>Servicii IT: virtualizare server consultantă, instalare/configurare software.</b>	buc	1	<p>Ofertantul va oferi servicii instalare și configurare precum: virtualizarea serverului pentru rularea corectă a următoarelor sisteme informaționale :</p> <ul style="list-style-type: none"> <li>• BitDefender Gravity Zone Enterprise Security;</li> <li>• Active Directory;</li> <li>• File Server;</li> <li>• Web Filtering pe grup de utilizatori pentru Firewall existent de model Watchguard și crearea politicilor de grup și utilizatori.</li> </ul> <p>Adițional, ofertantul va oferi servicii de instalare configurare și suport tehnic pentru:</p> <ul style="list-style-type: none"> <li>• Instalarea și configurarea BitDefender Enterprise Security – pentru 230 de PC-uri.</li> <li>• Configurarea AD - pentru cca 170 de utilizatori cu adăugarea stațiilor în Domain și migrarea informației existente.</li> <li>• Crearea politicilor și drepturilor de acces.</li> <li>• Realizarea unui raport cu lucrările efectuate în care se vor regăsi lucrările descrise mai sus;</li> </ul> <p><i>Notă:</i> Ofertantul va oferi servicii de training pentru administratorii IT din cadrul instituției.</p> <p>Beneficiarul va pune la dispoziția ofertantului softurile necesare.</p>		
<b>Lot 2</b>						
2	48000000-8	<i>Antivirus software</i>	buc	4	<p>Ofertantul va oferi o soluție de Antivirus de tip Bitdefender GravityZone sau echivalentul, prin achiziția a 4 licențe noi în scopul managementului centralizat pentru dispozitive de tip- Virtual Server. Instituția deține deja produsul Bitdefender GravityZone Enterprise Security. Licențele oferite trebuie să fie o completare la cele existente.</p> <p><u>Cantitatea</u>: Este responsabilitatea ofertantului de a determina modelul de licențiere și de acoperire a celor 230 licențe deja existente în cazul ofertării a unui alt produs, decât cel solicitat, care trebuie să fie conform cerințelor de mai jos:</p> <p>Se solicită o soluție de securitate centralizată pentru asigurarea unei protecții împotriva virușilor, a programelor spion, a mesajelor de tip spam, a tentativelor de fraudare de tip phishing și a altor coduri periculoase pentru 4 Virtual Server.</p> <p>Soluția furnizată trebuie:</p>	15000

			<ul style="list-style-type: none"> <li>•Să conțină o consola de management cu o baza de date inclusa care sa fie non-relaționala, pentru o funcționare cat mai rapida, fără a fi nevoie de licențe adiționale. Posibilitatea instalării și configurării de la distanță a tuturor componentelor antivirusului pentru stații de lucru din interiorul rețelei, precum și pentru generarea de rapoarte legate de acestea.</li> <li>•Pachetul de instalare va fi livrat ca o mașina virtuala bazata pe sistem de operare Linux securizat care conține toate rolurile sau serviciile necesare. Consola nu va necesita o licența suplimentara pentru sistemul de operare. Imaginea de tip „template” se va putea importa in: <ul style="list-style-type: none"> <li>-VMware vSphere</li> <li>-Citrix XenServer</li> <li>-Microsoft Hyper-V</li> <li>-Red Hat Enterprise Virtualization</li> <li>-KVM</li> <li>-Oracle VM.</li> </ul> </li> <li>•Soluția va fi scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașina virtuala.</li> <li>•Soluția va include adițional si un modul de balansare (load balancer) pentru cazurile in care mai multe mașini virtuale ale componentei de management sunt instalate cu același rol (pentru Load Balancing si performanta/redundanta).</li> <li>•Soluția va include un mecanism de configurare a disponibilității pentru serverul cu baze de date (clustering pentru redundanta). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe mașini virtuale.</li> <li>•Soluția trebuie sa aibă posibilitatea integrării cu Active Directory 2003 si versiuni mai recente.</li> <li>•Să ofere administratorilor de rețea posibilitatea identificării rapide a incidentelor legate de prezența unor programe periculoase și să poată aplica diverse politici de securitate.</li> <li>•Interfața consolei de management va fi obligatoriu in limba romana, adițional limba engleza si altele.</li> <li>•Interfața clientului de securitate, care se instalează pe stații si servere la fel va fi in limba romana, adițional limba engleza si altele.</li> <li>•Ofertantul va acorda manual de instalare si de administrare a produsului in limba romana.</li> </ul> <p>1) Cerințe minime obligatorii pentru componenta de securitate dedicata stațiilor de lucru :</p> <p>Soluția trebuie sa permită creșterea pe aceeași licența un număr nelimitat de dispozitive.</p> <p>Soluția trebuie sa includă:</p> <ul style="list-style-type: none"> <li>•scanare automată a fișierelor, a memoriei și a cheilor de regiștri Windows înainte de instalarea pe sisteme.</li> <li>•Soluția permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare trebuie sa includă actualizări de tip: ciclu rapid si ciclu lent.</li> <li>•Tehnologii de detectare, dezinfectare și trimitere în</li> </ul>
--	--	--	--

carantină a virușilor, programelor spion de tip adware/spyware, troienilor și rootkit-urilor, de asemenea detectarea atacurilor de tip zero-day de tip exploit (atacuri directionate).

- Posibilitatea de a programa scanări imediate sau la cererea utilizatorului pentru a evalua gradul de infectare al sistemului. Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fișiere mai mari de „ x ” MB, mărimea fișierelor putând fi definita de administratorul soluției, De asemenea posibilitatea definirii pana la minim 16 nivele de profunzime pentru scanarea in arhive.
- Produsul antimalware poate fi configurat sa folosească scanarea in Cloud si parțial scanarea locala.
- Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare, fie scanare locala sau scanare hybrida.
- Soluția oferă protecție in timp real pe mașinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.
- Soluția trebuie sa trimită în carantină fișierele suspecte sau infectate, în vederea reducerii riscului de propagare. Astfel administratorul va putea alege pentru fișiere infectate sau suspecte următoarele: interzice accesul, dezinfectează, ștergere, muta fișierele in carantina, nicio acțiune si alte acțiuni alternative.
- Protecție firewall individuală pentru utilizatorii de la distanță și ocazionali.
- Risc redus de infectare prin scanarea în timp real a traficului internet a tuturor stațiilor de lucru.
- Creșterea productivității și a nivelului de securitate prin blocarea accesului utilizatorilor la anumite site-uri ori prin blocarea posibilității de a transmite email-uri conținând date confidențiale.
- Colectarea de date despre amenințările informatice actuale de la toate stațiile de lucru și serverele din rețea cu ajutorul interfeței panoului de control.
- Management și configurare de la distanță, în conformitate cu politica de securitate.
- Configurarea, evaluarea, instalarea și îndepărtarea aplicațiilor la nivel de sistem.

Niveluri multiple de protecție avansată, soluția va permite configurarea setărilor anti malware prin intermediul politicilor din consola de management.

- Antivirus
- Antispam
- Antispyware
- Antiphishing
- Content Filtering
- Firewall.

- 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.
- Solutia permite aplicarea politicilor pe mașini client, grupuri de masini, domeniu, unitati organizationale.

			<ul style="list-style-type: none"> <li>•Pentru o mai buna protecție a stațiilor si serverelor, solutia trebuie sa includa un vaccin anti-ransomware. Acest vaccin va asigura protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea stațiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare.</li> <li>•Solutia va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware.</li> <li>•Vaccinul anti-ransomware primește actualizări de la producător, o dată cu actualizarea semnăturilor produsului Antimalware. Politica sa poate fi schimbata automat in funcție de: <ul style="list-style-type: none"> <li>a)User-ul logat pe statie</li> <li>b)IP sau clasa de IP al statiei</li> <li>c)Gateway-ul alocat</li> <li>d)DNS serverul alocat</li> <li>e)Clientul este/nu este in aceeași rețea cu infrastructura de management</li> <li>f)Tipul rețelei (lan, wireless)</li> </ul> </li> <li>•Actualizări automate a bazei de date ce conține semnături de viruși.</li> <li>•Soluția va permite stabilirea actualizării automate a consolei de management prin stabilirea graficilor zilnice, săptămânale sau lunare, dar si prin stabilirea intervalului orar in care acesta se va actualiza. De asemenea, permite si trimiterea unei alerte de ne funcționalitate, cu 30 de minute înainte de actualizare.</li> <li>•Soluția va dispune de un server de actualizare (update) care face posibila stabilirea componentelor ce vor fi descărcate automat de pe internet, fara intervenția administratorului. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor si serverelor pe care rulează sistemul de operare Windows, Linux, Mac.</li> <li>•Soluția permite stabilirea zonelor de test si critice din cadrul rețelei prin intermediul politicilor din consola de management</li> <li>•Pentru o urmărire amănunțita a actualizărilor consolei de management, soluția permite vizualizarea unui jurnal de modificări in care sunt precizate istoric: versiunea consolei de management; data versiunii; funcții noi si îmbunătățiri; probleme rezolvate; probleme cunoscute.</li> <li>•Soluția propusa va permite crearea unei copii de siguranța a bazei de date a consolei de administrare, la cerere sau programata, putând fi stocata local, pe un server FTP sau in rețea.</li> <li>•Soluția trebuie sa poată scana următoarele tipuri minime de sisteme: <ul style="list-style-type: none"> <li>-Procesor compatibil Intel® Pentium 1,6 MHz,</li> <li>Memorie RAM: 1 GB</li> <li>-Sistem de operare, baze de date si browser web:</li> <li>-Windows 7, 8.1, 10.</li> </ul> </li> <li>•Să existe posibilitatea ca în cazul trecerii la alt sistem de operare să fie livrat un kit de instalare și certificat de licență pentru produsul nou fără costuri suplimentare.</li> <li>•Posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice si/sau virtuale), servere (fizice si/sau virtuale).</li> </ul>	
--	--	--	---	--

			<p>•Pentru reducerea la minim a consumului de resurse, aplicația client antivirus trebuie să permită instalarea customizată a modulelor deținut.</p> <p>•Pentru a nu încălca resursele sistemului produsul antivirus trebuie să conțină un singur motor de scanare și să poată rula scanările programate cu prioritate redusă.</p> <p>2)Servicii solicitate Se vor asigura următoarele servicii:</p> <ul style="list-style-type: none"> <li>-Actualizarea bazei de semnături de virus și a motoarelor de scanare pe perioada întreaga perioadă.</li> <li>-In cazul în care în perioada de 12 luni de licențiere apare o versiune nouă a produsului, producătorul va pune la dispoziție versiunea nouă gratuit.</li> <li>-Distribuirea unor mesaje de atenționare de urgență prin e-mail în cazul apariției unor noi virusi distructivi sau cu potențial de răspândire rapidă,</li> <li>-Pentru orice virus pe care producătorul nu îl identifică și dezinfectează se va livra antidotul în cel mai scurt timp posibil de la trimiterea unei mostre a virusului.</li> <li>-Suport tehnic prin e-mail și mesagerie scrisă, non-stop 24/24 ore, 7/7 zile pe săptămâna, inclusiv în weekend și zilele de sărbătoare legale în limba română asigurat de către producătorul soluției, inclusiv suport din partea partenerului.</li> <li>-Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST).</li> </ul> <p><i>Notă:</i></p> <p>Luând în considerație faptul ca ANSA detine licența antivirus pentru 230 de utilizatori, în caz de oferire a altui produs decât Bitdefender, Ofertantul trebuie să acopere cu licență pentru toate 234 Device-uri (4 noi + 230 existente).</p>	
--	--	--	---	--

**Valoarea estimativă totală fără TVA**

**265000**

9. **În cazul în care contractul este împărțit pe loturi un operator economic poate depune oferta (se va selecta):** Pentru mai multe loturi;
10. **Admiterea sau interzicerea ofertelor alternative:** nu se admit.
11. **Termenii și condițiile de livrare/prestare/executare solicitați:** Maxim 30 de zile lucrătoare de la solicitare.
12. **Termenul de valabilitate a contractului:** 31.12.2019
13. **Contract de achiziție rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz):** nu
14. **Prestarea serviciului este rezervată unei anumite profesii în temeiul unor acte cu putere de lege sau al unor acte administrative (după caz):** nu
15. **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/Obligativitatea
1	Documentul Unic de Achiziții European	Formularul DUAE (anexa Nr.1 la Ordinul MF Nr.177 din 09.10.2018) semnat cu semnătură electronică.	Da
2	Dovada înregistrării persoanei juridice , în conformitate cu prevederile legale din Țara în care ofertantul este stabilit	Extras din Registrul de stat al persoanelor juridice (cu indicarea listei asociaților). Copie confirmată prin semnătură electronică	Da
3	Oferta	Specificații tehnice (Forma 4.1) Specificații de preț (Forma 4.2) – semnate cu semnătură electronică	Da
4	Raportul financiar	Ultimul raport financiar. Copie – confirmată prin semnătura electronică	Da
5	Formularul ofertei	Forma 3.1 - semnat cu semnătură electronică	Da
6	Certificat de atribuire a contului bancar eliberat de banca deținătoare de cont.	Copie confirmată prin semnătura electronică	Da
7	Certificat de efectuare regulată a plății impozitelor, contribuțiilor eliberat de Inspectoratul Fiscal	Copie confirmată prin semnătura electronică	Da
8	Autorizație de livrare a produsului de la producător	Copie – confirmată prin semnătura electronică	Da
9	Certificat tehnic a persoanelor certificate pe produsul oferat (minim 1)	Copie – confirmată prin semnătura electronică	Da
10	Garanția echipamentului minim 36 de luni pentru toate componentele hardware	Certificat de garanție, confirmat prin semnătura electronică	Da
11	Certificat ISO 9001:2015(Quality Management System)	Copie- confirmată prin semnătură electronică	Da
12	Certificat ISO 27001:2013 (Certificat de management al securității informației)	Copie- confirmată prin semnătură electronică	

**16. 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

**17. Condiții speciale de care depinde îndeplinirea contractului (indicați după caz):** Operatorul economic desemnat câștigător la lotul nr. 1 va oferi servicii de instalare și configurare a serverului

**18. Criteriul de evaluare aplicat pentru adjudecarea contractului:** cel mai mic preț

**19. Termenul limită de depunere/deschidere a ofertelor:**

- până la: *[ora exactă]* conform SIA RSAP
- pe: *[data]* conform SIA RSAP

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

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

**21. Termenul de valabilitate a ofertelor:** 35 zile

**22. Locul deschiderii ofertelor:** prin SIA RSAP

*Ofertele întârziate vor fi respinse.*



23. Persoanele autorizate să asiste la deschiderea ofertelor:  
*Ofertanții sau reprezentanții acestora au dreptul să participe la deschiderea ofertelor, cu excepția cazului când ofertele au fost depuse prin SIA "RSAP".*
24. Limba sau limbile în care trebuie redactate ofertele sau cererile de participare: limba de stat
25. Respectivul contract se referă la un proiect și/sau program finanțat din fonduri ale Uniunii Europene: nu
26. 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*
27. Data (datele) și referința (referințele) publicărilor anterioare în Jurnalul Oficial al Uniunii Europene privind contractul (contractele) la care se referă anunțul respective (dacă este cazul): -
28. Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț: nu a fost publicat
29. Data transmiterii spre publicare a anunțului de participare: \_\_\_\_\_
30. 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 | da                           |
| sistemul de comenzi electronice                                  | nu                           |
| facturarea electronică   | da                           |
| plățile electronice  | da                           |
31. Contractul intră sub incidența Acordului privind achizițiile guvernamentale al Organizației Mondiale a Comerțului (numai în cazul anunțurilor transmise spre publicare în Jurnalul Oficial al Uniunii Europene): nu
32. Alte informații relevante: \_\_\_\_\_

Conducătorul grupului de lucru: MALAI Ela

