

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: **Agencia 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
Lotul 1: Server pentru infrastructura de virtualizare si servicii de instalare						
1	48820000-2	Server	buc	1	<p><u>Cerințe generale:</u> 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, cadranul 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 - RAID levels 0, 1, 5, 6 - RAID spans 10, 50, 60 - Online Capacity Expansion (OCE)</p>	250000

- 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 drive and remote image mounting;
- SM & server diagnostics logging;

					<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> Garanția echipamentului minim 36 de luni pentru toate componentele hardware. Pentru administratorul IT din cadrul instituției se va organiza instruire de exploatare eficientă a sistemului. Ofertantul trebuie sa prezinte autorizație de livrare de la producator (Manufacturer's Authorization Form). Existenta accesului la un Centru de Deservire tehnica pentru deservirea echipamentului propus.</p>	
2	72000000-5	Servicii IT: virtualizare server consultantă, instalare/configurare software.	buc	1	<p>Ofertantul va oferi servicii instalare si configurare precum: virtualizarea serverului pentru rularea corectă a următoarelor sisteme informaționale :</p> <ul style="list-style-type: none"> • BitDefender Gravity Zone Enterprise Security; • Active Directory; • File Server; • Web Filtering pe grup de utilizatori pentru Firewall existent de model Watchguard și crearea politicilor de grup si utilizatori. <p>Additional, ofertantul va oferi servicii de instalare configurare si suport tehnic pentru:</p> <ul style="list-style-type: none"> • Instalarea si configurarea BitDefender Enterprise Security – pentru 230 de PC-uri. • Configurarea AD - pentru cca 170 de utilizatori cu adăugarea stațiilor in Domain și migrarea informației existente. • Crearea politicilor si drepturilor de acces. • Realizarea unui raport cu lucrarile efectuate in care se vor regasi lucrarile descrise mai sus; • Implementarea a unui sistem de backup la sistemele critice : 1C, Active Directory, File Server. • Crearea accesului din extern prin canale securizate utilizând Firewall-ul existent de model Watchguard pentru 15 utilizatori cu autentificarea conturilor din Active Directory. <p><i>Notă:</i> Ofertatul va oferi servicii de training pentru administratorii IT din cadrul instituției. Beneficiarul va pune la dispoziția ofertantului softurile necesare.</p>	
Lot 2: Antivirus software						
2	48761000-0	Antivirus software	buc	4	<p>Ofertantul va oferi o soluție de Antivirus de tip Bitdefender GravityZone sau echivalentul, prin achiziția a 4 licențe noi in scopul managementului centralizat pentru dispozitive de tip- Virtual Server. Instituția deține deja produsul Bitdefender GravityZone Enterprise Security. Licențele oferite trebuie sa fie o completare la cele existente.</p>	15000

Cantitatea: 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:

Se solicită o soluție de securitate centralizată pentru asigurarea unei protecții împotriva virusurilor, a programelor spion, a mesajelor de tip spam, a tentativelor de fraudare de tip phishing și a altor coduri periculoase pentru 4 Virtual Server.

Soluția furnizată trebuie:

- Să conțină o consolă de management cu o bază de date inclusă care să fie non-relațională, pentru o funcționare cât mai rapidă, 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.

- Pachetul de instalare va fi livrat ca o mașină virtuală bazată pe sistem de operare Linux securizat care conține toate rolurile sau serviciile necesare. Consola nu va necesita o licență suplimentară pentru sistemul de operare.

Imaginea de tip „template” se va putea importa în:

- VMware vSphere
- Citrix XenServer
- Microsoft Hyper-V
- Red Hat Enterprise Virtualization
- KVM
- Oracle VM.

- Soluția va fi scalabilă, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașină virtuală.

- Soluția va include adițional și un modul de balansare (load balancer) pentru cazurile în care mai multe mașini virtuale ale componentei de management sunt instalate cu același rol (pentru Load Balancing și performanță/redundanță).

- Soluția va include un mecanism de configurare a disponibilității pentru serverul cu baze de date (clustering pentru redundanță). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe mașini virtuale.

- Soluția trebuie să aibă posibilitatea integrării cu Active Directory 2003 și versiuni mai recente.

- Să ofere administratorilor de rețea posibilitatea identificării rapide a incidentelor legate de prezența unor programe periculoase și să poată aplica diverse politici de securitate.

- Interfața consolei de management va fi obligatoriu în limba română, adițional limba engleză și altele.

- Interfața clientului de securitate, care se instalează pe stații și servere la fel va fi în limba română, adițional limba engleză și altele.

- Ofertantul va acorda manual de instalare și de administrare a produsului în limba română.

1) Cerințe minime obligatorii pentru componenta de securitate dedicată stațiilor de lucru :

Soluția trebuie să permită creșterea pe aceeași licență un număr nelimitat de dispozitive.

Soluția trebuie să includă:

- scanare automată a fișierelor, a memoriei și a cheilor de regiștri Windows înainte de instalarea pe sisteme.
- Soluția permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare trebuie să includă actualizări de tip: ciclu rapid și ciclu lent.
- Tehnologii de detectare, dezinfectare și trimitere în 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 automată în timp real va putea fi setată să nu scaneze arhive sau fișiere mai mari de „ x ” MB, mărimea fișierelor putând fi definită de administratorul soluției, De asemenea posibilitatea definirii până la minim 16 nivele de profunzime pentru scanarea în arhive.
- Produsul antimalware poate fi configurat să folosească scanarea în Cloud și parțial scanarea locală.
- Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare, fie scanare locală sau scanare hibridă.
- Soluția oferă protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată.
- Soluția trebuie să 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 în carantină, nicio acțiune și 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 masini client, grupuri de masini, domeniu, unitati organizationale.
- Pentru o mai buna protectie a statiilor si serverelor, solutia trebuie sa includa un vaccin anti-ransomware. Acest vaccin va asigura protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea statiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare.
- Solutia va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware.
- Vaccinul anti-ransomware primește actualizări de la producător, o dată cu actualizarea semnăturilor produsului Antimalware. Politica sa poate fi schimbata automat in functie de:
 - a)User-ul logat pe statie
 - b)IP sau clasa de IP al statiei
 - c)Gateway-ul alocat
 - d)DNS serverul alocat
 - e)Clientul este/nu este in aceeași rețea cu infrastructura de management
 - f)Tipul rețelei (lan, wireless)
- Actualizări automate a bazei de date ce conține semnături de viruși.
- 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.
- 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.
- Soluția permite stabilirea zonelor de test si critice din cadrul rețelei prin intermediul politicilor din consola de management
- 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.
- Soluția propusa va permite creare 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.
- Soluția trebuie sa poată scana următoarele tipuri minime de sisteme:

-Procesor compatibil Intel® Pentium 1,6 MHz, Memorie RAM: 1 GB

			<p>-Sistem de operare, baze de date si browser web: -Windows 7, 8.1, 10.</p> <ul style="list-style-type: none"> •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. •Posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice si/sau virtuale), servere (fizice si/sau virtuale). •Pentru reducerea la minim a consumului de resurse, aplicația client antivirus trebuie să permită instalarea customizată a modulelor deținut. •Pentru a nu încărca resursele sistemului produsul antivirus trebuie să conțină un singur motor de scanare și să poată rula scanările programate cu prioritate redusă. <p>2)Servicii solicitate</p> <p>Se vor asigura următoarele servicii:</p> <ul style="list-style-type: none"> -Actualizarea bazei de semnături de virus si a motoarelor de scanare pe perioada întreaga perioadă. -In cazul in care in perioada de 12 luni de licențiere apare o versiune noua a produsului, producătorul va pune la dispoziție versiunea noua gratuit. -Distribuirea unor mesaje de atenționare de urgență prin e-mail in cazul apariției unor noi virusi distructivi sau cu potențial de răspândire rapida, -Pentru orice virus pe care producătorul nu îl identifică și dezinfectează se va livra antidotul in cel mai scurt timp posibil de la trimiterea unei mostre a virusului. -Suport tehnic prin e-mail si mesagerie scrisă, non-stop 24/24 ore, 7/7 zile pe săptămâna, inclusiv in weekend si zilele de sărbătoare legale in limba română asigurat de către producătorul soluției, inclusiv suport din partea partenerului. -Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST). -Ofertantul va prezenta autorizarea de la producător pentru produsul livrat. -Ofertantul va prezenta minim 1 certificat tehnic a persoanelor certificate pe produsul oferit. <p><u>Notă:</u></p> <p>Luând in considerație faptul ca ANSA detine licența antivirus pentru 230 de utilizatori, in caz de oferire a altui produs decât Bitdefender, Ofertantul trebuie sa acopere cu licență pentru toate 234 Device-uri (4 noi + 230 existente).</p>	
--	--	--	---	--

Valoarea estimativă totală fără TVA

265000,00

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 (DUAЕ, documentație):**

Nr. d/o	Descrierea criteriului/cerinței	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/Obligativitatea
1	Documentul Unic de Achiziții European	Formularul DUAЕ (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 ISO 9001:2015(Quality Management System)	Copie- confirmată prin semnătură electronică	Da
10	Certificat ISO 27001:2013 (Certificat de management al securității informației)	Copie- confirmată prin semnătură electronică	Da
13	Demonstrarea accesului la personalul necesar pentru îndeplinirea corespunzătoare a obiectului contractului ce urmează a fi atribuit (personalul de specialitate care va avea un rol esențial în îndeplinirea acestuia).	Pentru Lot 1 si Lot. 2 – Ofertantul va prezenta minim 2 certificate tehnice a persoanelor certificate pe produsul de antivirus.	Da

- 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 si 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:

Ela MALAI

L.Ș.