ANUNȚ DE PARTICIPARE

privind achiziționarea
„Licență antivirus"
prin procedura de achiziție publică de valoare mică

1. **Denumirea autorității contractante:** Administrația Națională a Penitenciarelor
2. **IDNO:** 1006601001012
3. **Adresa:** mun. Chișinău, str. N. Titulescu 35
4. **Numărul de telefon/fax:** 022 - 409 -709 / 022 - 409 -748
5. **Adresa de e-mail și de internet a autorității contractante:** anp@anp.gov.md / http://anp.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* – anastasia.ionel@anp.gov.md
7. **Tipul autorității contractante și obiectul principal de activitate (dacă este cazul, menționea că autoritatea contractantă este o autoritate centrală de achiziție sau că achiziția implică o altă formă de achiziție comună):** Instituție de stat cu statut special
8. **Procedura a fost inclusă în planul de achiziții publice a autorității contractante:** Da
   Link-ul către planul de achiziții publice publicat:
   https://drive.google.com/drive/folders/17c0bNPOunoSaPY87vLnuSI32KiPaDOdO

Cod CPV	Nr. d/o	Denumirea bunurilor solicitate	Unitatea de măsură	Cantitatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată (se va indica pentru fiecare lot în parte) fără TVA
48761000-0	1	**Licență Antivirus**	Buc.	210	Soluție de protecție și securitate antivirus pentru protecția infrastructurii: Se solicită prelungirea mentenanței anuale a soluției corporative antivirus deja existente în cadrul instituției pentru o perioadă de 12 luni: - WithSecure Elements EPP for Computers Premium, Company Managed License, renewal, 12 luni pentru 182 stații de lucru fizice și virtualizate; - WithSecure Elements EPP for Servers Premium, Company Managed License, renewal, 12 luni, pentru 3 servere fizice și virtualizate; - WithSecure Elements Vulnerability Management, Company Managed License, 12 luni subscriptie, pentru 25 hosturi fizice și virtualizate. Soluția de securitate ofertată trebuie să se regăsească în Gartner în ultimii 4 ani de zile și să ocupe locuri de top în testele internaționale "AV-TEST" cel puțin 8 ani la rînd.	**58 400,00 lei**
	TOTAL					**58 400,00 lei**

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:**

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

11. **Admiterea sau interzicerea ofertelor alternative:** se admite. În cazul în care ofertantul dorește să ofere un produs alternativ decât cel existent, acesta trebuie să întrunească minim cerințele de mai jos, echivalent soluției instalate deja in cadrul instituției:

1.1. Cerințele tehnice funcționale minim solicitate față de Soluția antivirus pentru protecția stațiilor de lucru și a serverelor:
Soluția trebuie să asigure protecție și management centralizat pentru stații de lucru, servere și dispozitive mobile care să

acopere urmatoarele sisteme de operare:

Stații de lucru:

- Microsoft Windows 7 Service Pack 1; 8.1; 10 ,11; (all 32-bit and 64-bit editions);

Servere:

- Microsoft® Windows Server 2008 R2
- Microsoft® Small Business Server 2011, Standard edition
- Microsoft® Small Business Server 2011, Essentials
- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2012 Essentials
- Microsoft® Windows Server 2012 R2
- Microsoft® Windows Server 2012 R2 Essentials
- Microsoft® Windows Server 2012 R2 Foundation
- Microsoft® Windows Server 2016 Standard
- Microsoft® Windows Server 2016 Essentials
- Microsoft® Windows Server 2016 Datacenter
- Microsoft® Windows Server 2016 Core
- Microsoft® Windows Server 2019 Standard
- Microsoft® Windows Server 2019 Essentials
- Microsoft® Windows Server 2019 Datacenter
- Microsoft® Windows Server 2019 Core
- Microsoft Windows Server 2022 Standard
- Microsoft Windows Server 2022 Essentials
- Microsoft Windows Server 2022 Datacenter
- Microsoft Windows Server 2022 Core

Servere Terminale:

- Microsoft Windows Terminal/RDP Services (on the above mentioned Windows Server platforms)
- Citrix® XenApp 5.0
- Citrix® XenApp 6.0
- Citrix® XenApp 6.5
- Citrix® XenApp 7.5, 7.6, 7.14, 7.15
- Citrix® Virtual Apps and Desktops 2009

Linux:

- AlmaLinux 8
- Amazon Linux 2
- CentOS 7 (7.3 or newer)
- CentOS 8
- CentOS Stream 8
- Debian 9
- Debian 10
- Debian 11 (with no SELinux enabled)
- Oracle Linux 7
- Oracle Linux 8
- RHEL 7 (7.3 or newer)
- RHEL 8
- SUSE Linux Enterprise Server 12
- SUSE Linux Enterprise Server 15
- Ubuntu 16.04
- Ubuntu 18.04
- Ubuntu 20.04

Dispozitive Mobile:

- Android 7.0 (Nougat) sau mai sus; iOS 12.1 sau mai sus, iPadOS 13 sau mai sus, care sa ofere browsing protection separat securizat, mobile VPN pentru protecția personală, protecție malware cel puțin pentru Android.

Soluția trebuie să ofere următoarele funcționalități

- Soluția ofertată trebuie să fie una bazată pe tehnologia Cloud, care să ofere un management centralizat a tuturor dispozitivelor: stații de lucru, servere și dispozitive mobile;
- Soluția trebuie sa asigure protecție in timp real, impotriva virusilor (ransomware – crypto) cu scopul prevenirii distrugerii și modificării datelor, amenintarilor spyware, rootkit-urilor, tentativelor de intruziune, spam-urilor si a altor mesaje nedorite.
- Soluția trebuie să ofere actualizari automate a versiunilor noi si a hotfix-urilor;
- Soluția trebuie să ofere protectie impotriva virusilor si noilor amenintari necunoscute care să fie bazată pe analize euristice, de comportament și reputație;
- Soluția trebuie să includă patch management cu opțiuni pentru excluderi și actualizări manuale;
- Soluția trebuie să ofere statistica pentru urmatoarele: top patch-uri instalate,severitatea patch-urilor, top vendori dupa cantitatea actualizarilor.
- Soluția trebuie să ofere posibilitatea de a crea politici de securitate ce vor fi distribuite la discreția administratorului.
- Soluția trebuie să ofere posibilitatea de a compara una sau mai multe politici de securitate.
- Soluția trebuie să ofere posibilitatea de a stabili politica implicita pentru calculatoare , servere , dispozitive mobile ,

linux , macOS.
- Soluția trebuie să ofere funcționalități de firewall, intrusion prevention, application control si sanbox pentru analiza traficului de tip ransomware și detonarea acestuia;
- Soluția trebuie să asigure criptarea automată prin VPN, a întregului trafic realizat dintre dispozitivele mobile, permițând utilizarea în condiții de siguranță a Wi-Fi public și rețelelor mobile;
- Soluția trebuie să ofere posibilități exacte de activare și dezactivare, de configurare a funcționalităților precum: scanarea antivirus la cerere, firewall gestionat, controlul accesului la Internet, controlul aplicațiilor care să blocheze executarea aplicațiilor și scripturilor conform regulilor create sau definite de administrator, scanarea traficului web, controlul dispozitivelor;
- Soluția trebuie să ofere posibilitatea de a scana calculatoarele din Active Directory, ce nu sunt protejate de agentul de securitate.
- Soluția trebuie sa ofere posibilitatea de a descarca agentul de securitate in format de tip .msi pentru ulterioara implementare in AD.
- Soluția trebuie sa ofere posibilitatea de a transmite invitatie pe email, pentru descarcarea agentului de securitate cu licenta integrata;
- Soluția trebuie să ofere instalare centralizată a stațiilor de lucru și terminalelor mobile;
- Soluția trebuie să ofere posibilitatea de a activa pentru utilizatori dubla autentificare.
- Soluția trebuie să ofere functional Multi-engine anti-malware;
- Soluția trebuie să includă funcționalul de Patch Management, pentru a asigura actualizarea de software atît de la produsele Microsoft, cît și pentru alte aplicații de la terți;
- Soluția trebuie să ofere posibilitatea vizualizarea istoriilor instalarilor a aplicatiilor sau actualizarilor invechite minim continind urmatoarele date: timpul instalarii , vendor , aplicatie , versiunea instalata , versiunea anterioara instalata , numele calculatorului , statutul instalarii , criticitatea actualizarii , CVE ID , Bulletin ID. Posibilitatea filtrarii dupa: categorii de actualizari , perioada , statut , tipul de platforma. Posibilitatea de a exporta informatia in CSV fisier.
- Soluția trebuie să ofere funcțional de Firewall ce va permite setarea unor reguli bazate pe acțiuni (blocarea sau permiterea) și direcție(intrare sau iesire) pentru controlul și monitorizarea traficului la nivel de endpoint și rețea, care să furnizeze un nivel de securitate suplimentar, aflat deasupra regulilor utilizatorului pentru Windows Firewall și a altor reguli pentru domenii.
- Soluția trebuie să ofere funcțional de Protecție Web: protejarea accesarilor pe site-uri bancare (Control conexiune) care să alerteze utilizatorii atunci când aceștia au o conexiune securizată către site-uri de operațiuni bancare online și către alte site-uri precizate care tratează informații sensibile; blocarea site-urilor cunoscute ca fiind dăunătoare (Navigare bazată pe reputație); împiedicarea accesului la site-urile nepermise (Controlul conținutului Web); blocarea accesului la tipurile de conținut nepermise (Filtrare tipuri de conținut).;
- Soluția trebuie să ofere funcțional de Controlul conexiunilor prin securizarea plăților online si afisarea unui pop-up care blocheaza celelalte pagini si imposibilitate accesarii altor decat cea in care se efectueaza tranzactia , posibilitatea de a bloca conexiunile de la distanta (cu posibilitatea de a adauga in excludere dupa IP) , blocarea liniei de comanda si a instrumentelor de scriptare
- Soluția trebuie să ofere funcțional de scanare în timp real a tuturor obiectelor pe care le accesează utilizatorii finali, pentru depistarea programelor de tip malware și inclusiv să ofere posibilitatea de configurare și efecuare a scanării manuale;
- Soluția trebuie să ofere funcțional de scanare a aplicațiilor în cloud;
- Soluția trebuie să ofere funcțional de Scanare a semnăturilor;
- Soluția trebuie sa ofere posibilitatea de a expedia invitații pentru instalarea agentului de securitate minim in limba româna , rusa , engleza si cu posibilitatea de a importa mai multe cutii postale printr-un fisier de tip CSV. Vizualizarea invitatiilor expediate/expirate si posibilitatea de a reaminti utilizatorul printr-un email de a instala Soluția de protectie.
- Soluția trebuie să ofere posibilitatea de a importa/exporta politica de securitate si blocarea modificarilor in politica.
- Soluția trebuie sa ofere posibilitatea de a seta scanarea programata (zilnic , saptaminal , lunar)
- Soluția trebuie să ofere posibilitatea de a scana fisierele de tip ZIP , RAR...
- Soluția trebuie sa ofere posibilitatea de a scana fisierele de tip mailbox PST , OST...
- Soluția trebuie să permită activarea/dezactivarea modulelor de securitate, bazată de locația identificată a dispozitivului dupa urmatoarele criterii: DNS server ip address , DHCP server ip address , default gateway ip address, wins ip address.
- Soluția trebuie să ofere procese automatizate precum: scanare rapidă pentru malware , scanare programată pentru malware , restart forțat , oprire forțată , hibernare , instalarea actualizarilor de securitate critică și importantă , instalarea tuturor actualizarilor.
- Soluția trebuie să includă funcțional de control a dispozitivelor externe, să ofere posibilitatea: de a seta restricții în privința modului în care utilizatorii pot accesa urmatoarele dispozitive: USB Mass Storage Devices , Bluetooth Devices , IrDA Devices , IEEE 1394 Host Bus Controllers , Imaging Devices (cameras and scanners) , Smart Card Readers , COM & LPT ports , Modems , Floppy drives , Windows CE ActiveSync devices , DVD/CD-ROM drives , Wireless devices , Imprimante; de a interzcie accesul la orice dispozitiv de stocare USB; de a stopa rularea executabilelor stocate pe astfel de dispozitive; de a seta restricții pe grupuri de dispozitive;
- Soluția trebuie să ofere funcțional de analiză euristică si zero day, de comportament și reputație;
- Soluția trebuie să ofere funcțional de Sandbox automatizat inclus – pentru analiza amănunțită prin detonarea fișierilor malițioase sau care nu pot fi protejate in baza de semnătura sau comportament;
- Soluția trebuie să ofere funcțional de control al aplicatiilor, prin setarea unor reguli de blocare create ca excluderi pentru a bloca un acces anume și să fie bazate:
- pe actiuni precum permiterea, blocarea, sau permiterea și monitorizarea aplicațiilor;
- pe evenimente precum pornire aplicație, încărcare modul, pornire program de instalare, acces la fișiere, pornire aplicație și încărcare modul;

- prin stabilirea unor condiții care să poată fi selectate după atribute (cale destinație, nume fișier destinație, reputație destinație, versiune fișier destinație, cod hash pentru certificat la destinație, etc), condiție și valoare, ce vor asigura activarea regulilor de excludere;
- Soluția trebuie să ofere funcțional de Management API prin integrarea solutiilor terte precum: SIEM/RMM;
- Soluția trebuie sa ofere posibilitatea de dezinstalare a agentului de securitate de la distanta;
- Soluția trebuie să ofere posibilitatea de a transmite un mesaj informativ pe statiile distante;
- Soluția trebuie să ofere posibilitatea de izolare a statiilor de la distanță;
- Soluția trebuie să ofere posibilitatea de a șterge din carantină fisierelor malițioase identificate, restabilirea fisierelor malitioase la locatia originară, excluderea fisierului dupa calea deplina, excluderea fisierului dupa SHA1;
- Soluția trebuie să ofere posibilitatea de a descarca evenimentele de securitate in format (JSON);

1.1. Cerintele tehnice vis-a-vis de administrarea solutiei antivirus:

- administrarea soluției ofertate este necesara să se faca printr-o singură consolă de administrare bazată pe cloud, fără ca să necesite creva echiapmente hardware (servere de management) sau careva software special.
- consola de administrare trebuie să fie capabilă de a funcționa pe orice dispozitiv și să conțină toate funționalitățile sus solicitate;
- posibilitatea administrării centralizare, prin intermediul unei singure console, a urmatoarelor medii și funcționalități: stații de lucru fizice și virtualizate, servere fizice și virtualizate, dispozitivelor mobile pe Android si iOS, iPadOS, căsuțelor poștale pe Exchange sau office 365, scanarea vulnerabilitatilor web și a infrastructurii IT (interne și externe), scanarea dispozitivelor la anomalii, investigarea lor în detaliu și stoparea scurgerilor de date;
- să suporte următorele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari;
- interfața consolei a clientului trebuie să asigure posibilitatea de funcționare în limbile: romana, rusă si engleză obligatoriu, cu capacitatea de a putea fi selectată limba dorită, în scopul unei administrări mai ușoare de către administratori;
- administratorul trebuie să poată permite sau interzice utilizatorului de a activa sau dezactiva caracteristicile de securitate setate;

1.2. Cerințe vis-a-vis de funcționalul de raportare și alerte a solutiei antivirus:

- Soluția trebuie să permită generarea de rapoarte grafice detaliate, saptămînal sau lunar, cu posibilitate de export minimum in format (csv), inclusiv cu remitere automată către adrese de email specificate, rapoartele trebuie să cuprindă minim informație despre:

*Top de infecții tratate;
*Infecții gestionate;
*Starea de protecție;
*Cele mai recente actualizări pentru definițiile de malware pe computere;
*Dacă s-au instalat actualizările de securitate;

- Soluția trebuie să permită setarea și configurarea de alerte, declanșarea lor să poată fi aplicată pentru minim următoarele acțiuni: blocat, redenumit, oprit, șters, plasat, raportat, dezinfectat, în carantină, raportat către utilizator, blocat și acțiune suplimentară solicitată de la utilizator, mutat în coșul de gunoi si ulterior expediata catre o cutie postala sau mai multe.
- Soluția, prin intermediul direct al experților producătorului, trebuie să oferă consultanță și expertiză în materie de securitate cibernetică și să fie disponibili ca serviciu prin intermediul funcției de produs încorporat în consolă sub SLA cu un minim de 2 ore și acces la ei 24/7/365.
- Soluția va oferi un serviciu avansat de căutare și răspuns la amenințări prin intermediul consolei, accesând inclusiv la direct suportul producătorului.

1.3 Cerințele tehnice funcționale minim solicitate față de Soluția de scanare a vulnerabilităților a infrastructurii interne, externe si web:

-Produsul ofertat va trebui să poată fi extins prin achiziția ulterioară a unei soluții de antivirus, de la același producător pentru a exista o integrare nativă a soluției. Cu posibilitatea de a accesa dintr-o singură interfață fie Soluția de antivirus fie soluția de scanare a vulnerabilităților.
-Platforma trebuie să fie capabilă să identifice atât amenințările interne cît și pe cele externe și să raporteze riscurile și reglementările conform minim PCI, GDPR.
-Soluția trebuie să asigure scanarea vulnerabilităților pentru echipamente din rețea, aplicațiilor web, site-urilor interne sau externe.
- Soluția ofertată trebuie să fie una bazată pe tehnologia Cloud, care să ofere o vizibilitate a vulnerabilităților într-un mod centralizat pentru toate tipurile de dispozitive conectate în rețea si care pot comunica, de exemplu: stații de lucru, servere, servere virtuale, site-uri, switch-uri, routere, aplicațiilor web, etc;
- Soluția va oferi posibilitatea de a identifica toate echipamentele conectate la rețea, la fel va fi posibil de a verifica tipul de echipament, după caz: sistemul de operare instalat, IP-ul si MAC adresa, a cărui domeniu se atribuie, vulnerabilitățile depistate, software-ul instalat pe echipament, spațiu disponibil, tipul procesor, tip de Bios.
- Soluția va permite planificarea activităților după data/ora/an și de rulat scanarea vulnerabilităților pentru fiecare echipament in parte.
- Soluția va pune la dispoziție un instrument care poate fi instalat pe o mașină virtuală sau pe un calculator in rețeaua pe care se dorește o scanare al vulnerabilităților sau pentru colectarea datelor echipamentelor aflate in rețea.
- Soluția trebuie sa permită adăugarea unui grup de scanare in care se va indica minim: Numele grupului si persoana responsabilă, descrierea succintă a grupului.
- Posibilitatea de scanare prin alegerea unui șablon prestabilit care va propune de a scana sistemul după minim următoarele modele:

• TCP 0-65535 , UDP 0-1024
• Badlock detection
• Bash Shellshock detection

• GHOST detection
• Hearbeast detection
• Limited TCP 0-30000, no UDP
• PCI scan
• Scan full TCP/UDP port range
• Scan top-100 ports
• Scan top-1000 ports
• SSL/TLS maturity scanning
- Modul de scanare să poată fi setat după: oră, repetări zilnice, săptămânale, lunare, trimestriale, etc.
- Soluția trebuie să ofere funcțional de Management API prin integrarea soluțiilor terțe;
- Soluția trebuie să ofere posibilitatea de setare a unui logo care trebuie să se afișeze in consola de administrare și în rapoartele de vulnerabilități exportate.
- Soluția va dispune de posibilitatea de autentificare prin doi factori cu ajutorul unor soluții bazate pe TOTP (Time-based One Time Password) ca:
• Google Authenticator,
• Microsoft Authenticator,
• Sau altele care suportă acest algoritm.
- Administrarea soluției este necesară să se facă printr-o singură consolă de administrare bazată pe cloud, fără ca să necesite careva echipamente hardware(servere de management) sau careva software speciale.
-Soluția propusă trebuie sa poată genera un raport pe segmente din rețea pe care se dorește. Si va fi posibil de a selecta ce fel de vulnerabilități să fie afișate in raport, sortate după severitatea lor.
-Soluția propusă trebuie să pună la dispoziție posibilitatea de a asigna remedierea unei vulnerabilități către un user / administrator creat in platforma de administrare.
-Asignarea unui task va fi posibil prin crearea unui ticket astfel se va indica unele date ca : denumire task, descrierea succintă, perioada până când să fie executat, prioritatea, o perioadă estimată pentru remediere, etc.
-Soluția trebuie să dispună de capacitatea de a automatiza unele procese de lucru ca:
- Închiderea si redeschiderea automată a tichete-lor;
- Să transmită notificări tuturor participanților la expirarea taskului;
- Până la expirarea termenului limită pentru executarea taskului, Soluția va notifica toți participanții.
- Consola de administrare trebuie să suporte următoarele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari;
- Interfața consolei de administrare trebuie să asigure posibilitatea de funcționare cel puțin în limba engleză obligatoriu.
- Soluția va permite accesul altor useri cu drepturi de: administrator, doar vizualizare sau colegi de echipă.
- Soluția va putea afișa toată informația referitor la licența instalată, jurnal de evenimente, modificările aplicate de către user-ul care are accesul la portal.
- In consola de administrare trebuie sa se regăsească acces la manuale, ghiduri de instalare, ghidul de utilizare, etc, informații referitor la schimbările si actualizările soluției, comunitate, portal pentru suport cu posibilitatea de a solicita ajutor de la producător.
- Soluția trebuie să asigure lipsa actualizărilor de software și patch-uri care sunt afișate în consola de administrare cu ID-uri CVE și link către baza de date de vulnerabilitate și expunere comună (CVE) pentru informații suplimentare despre detaliile și criticitatea vulnerabilității
- Soluția trebuie să ofere o modalitate de a executa scanări autentificate pe sistemele țintă
- Soluția trebuie să ofere scanările de descoperire trebuie să fie nelimitate pe parcusul perioadei de licență.
- Soluția trebuie să ofere activarea accesului catre date prin configurarea cheilor API
- Soluția trebuie să fie customizabilă pentru scanări, performanță, șabloane și rapoarte.

1.3.1 Cerințe față de funcționalul de raportare și alerte a sistemului de scanare a vulnerabilitatilor:

- Soluția trebuie să permită generarea de rapoarte grafice detaliate, cu posibilitate de export minim in format (docx.xml,xlsx), inclusiv cu remitere către adrese de email specificate. Posibilitatea de a configura o frecventa pentru crearea rapoartelor dupa (zi , săptămâna, luna, ora), rapoartele trebuie să cuprindă minim informație despre:
* Vulnerabilitățile descoperite clasificate după severitate: informativ, severitate minimă, severitate medie, si severitate înalta.
* Notarea severității vulnerabilităților se va face pe notă de la 1 la 10
* Raportul va afișa descrierea pentru fiecare vulnerabilitate in parte cu unele referințe.
* Recomandările propuse pentru remedierea vulnerabilității depistate.
* Crearea unei statistici grafice in dependență de vulnerabilitățile depistate
* Top vulnerabilități depistate.
- Soluția trebuie să permită crearea unor widgeturi care pot fi editate, clonate sau șterse cu afișarea lor pe pagină in mod dinamic. La fel, widgeturi de bord pot fi create in forma de minima de: tabel, plăcinta, histograma, etc.
- Tablourile de bord trebuie să conțină informații ca: vulnerabilitățile depistate care vor fi grupate după severitate/data/luna/cantitatea depistată. Cele mai grave vulnerabilități. Scanările active, scanările care sunt planificate, ultimele dispozitive scanate.

Soluția trebuie să permită setarea și configurarea de alerte, declanșarea lor să poată fi aplicată pentru minim următoarele acțiuni: când startează un proces de scanare, finalizarea procesului de scanare, la crearea si asignarea unui task către un utilizator existent.

12.Termenii și condițiile de livrare/prestare/executare solicitați: 10 zile lucrătoare de la data intrării în vigoare a contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției., mun. Chișinău, str. N. Titulescu, 35

13.Termenul de valabilitate a contractului: 31.12.2022

14.Contract de achiziție rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz): Nu

15.Prestarea serviciului este rezervată unei anumite profesii în temeiul unor acte cu putere de lege sau al unor acte administrative (după caz): Nu

16.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	Denumirea documentului/cerinţei	Cerinţe suplimentare faţă de document	Obligativitatea
1.	Oferta	- confirmat prin semnătura electronică a Participantului (conform anexei);	Da
2.	Informaţii generale despre ofertant (sediul ofertantului şi al filialelor acestuia)	- confirmat prin semnătura electronică a Participantului(format liber);	Da
3.	Dovada înregistrării juridice	- confirmat prin semnătura electronică a Participantului	Da
4.	Certificat de atribuire al contului bancar	- eliberat de banca deţinătoare de cont - confirmat prin semnătura electronică a Participantului	Da
5.	Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul ofertat.	-emis de organul abilitat – copie confirmată prin ştampila şi semnătura participantului sau semnat electronic.	Da
6.	Autorizarea de la producător pentru licitatia la care participa ofertantul.	- confirmat prin semnătura electronică a Participantului	Da
7.	Certificat tehnic pe solutiile propuse.	- Prezentarea a minim 2 certificate, confirmate prin semnătura electronică a Participantului	Da
8.	Certificata in calitate de auditor intern pentru sistemul de management al securităţii informaţionale conform ISO 27001:2013	- confirmat prin semnătura electronică a Participantului, pentru minim o persoană angajată a ofertantului	Da
9.	Minim 3 referinţe şi 3 recomandări de implementare pe piaţa locală a soluţiei ofertate.	- confirmat prin semnătura electronică a Participantului,	Da
10.	*Alte acte sau declaraţii pe propria răspundere, după caz ce confirmă:* 1. Pentru Soluţia ofertată se solicită a fi 12 luni suport local şi de la producător. 2. Producătorul trebuie să ofere suport 24/7, prin e-mail sau conectare de la distanţă, inclusiv suport local din partea partenerului. Necesar de prezentat timpii de reacţie ofertat. 3. Lucrările de instalare, configurare, punerea în funcţiune a soluţiei trebuie să fie executate de ofertant, iar costul acestora trebuie să fie incluse în oferta comerciala.	- confirmat prin semnătura electronică a Participantului,	Da

În situaţia identificării de către ANP a diferenţei între suma preţurilor unitare şi preţul total din oferta, urmează ***a fi luat în calcul preţul unitar fără TVA****, iar suma totală va fi corectată corespunzător, fiind coordonată în prealabil cu operatorul economic.* ***Preţul ofertat per unitate, după virgulă va fi rotunjit până la zecimi****. Dacă ofertantul nu va accepta corecţia acestor erori, oferta, în consecinţă, va fi respinsă.*

17. 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 în 3 runde cu pasul minim 1%

18. Condiții speciale de care depinde îndeplinirea contractului (indicați după caz): -

19. Criteriul de evaluare aplicat pentru adjudecarea contractului: cel mai mic preț fără TVA și corespunderea specificației tehnice solicitate

20. Factorii de evaluare a ofertei celei mai avantajoase din punct de vedere economic, precum și ponderile lor:

Nr. d/o	Denumirea factorului de evaluare	Ponderea%
-	-	-

21.Termenul limită de depunere/deschidere a ofertelor:
conform SIA RSAP MTender (https://mtender.md/)

22.Adresa la care trebuie transmise ofertele sau cererile de participare:
Ofertele sau cererile de participare vor fi depuse electronic prin intermediul SIA RSAP

23.Termenul de valabilitate a ofertelor: 30 zile din data limită de depunere a ofertelor

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

25.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".

26.Limba sau limbile în care trebuie redactate ofertele sau cererile de participare: română

27.Respectivul contract se referă la un proiect și/sau program finanțat din fonduri ale Uniunii Europene: nu

28.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

29.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): nu

30.În cazul achizițiilor periodice, calendarul estimat pentru publicarea anunțurilor viitoare: anul 2022

31.Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț: nu a fost publicat

32.Data transmiterii spre publicare a anunțului de participare: 01.07.2022

33.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	-
facturarea electronică	-
plățile electronice	-

34. 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

35. Alte informații relevante: nu sunt

Conducătorul grupului de lucru:

L.Ș.

Cod CPV		Denumirea serviciilor	Cantitatea	Preț unitar (fără TVA)	Preț unitar (cu TVA)	Suma fără TVA	Suma cu TVA	Specificația tehnică solicitată de către autoritatea contractantă	Specificația tehnică deplină propusă de ofertant	Termenul/locul de livrare	Clasificat bugetar (IBAN
48761000-0	1	**Licență Antivirus**	210 buc.					Soluție de protecție și securitate antivirus pentru protecția infrastructurii: Se solicită prelungirea mentenanței anuale a soluției corporative antivirus deja existente în cadrul instituției pentru o perioadă de 12 luni: - WithSecure Elements EPP for Computers Premium, Company Managed License, renewal, 12 luni pentru 182 stații de lucru fizice și virtualizate; - WithSecure Elements EPP for Servers Premium, Company Managed License, renewal, 12 luni, pentru 3 servere fizice și virtualizate; - WithSecure Elements Vulnerability Management, Company Managed License, 12 luni subscriptie, pentru 25 hosturi fizice și virtualizate. Soluția de securitate ofertată trebuie să se regăsească în Gartner în ultimii 4 ani de zile și să ocupe locuri de top în testele internaționale "AV-TEST" cel puțin 8 ani la rînd.		10 zile lucrătoare de la data intrării în vigoare a contractului, care include și tipul lucrărilor de instalare, configurare și punerea în funcțiune a soluției., mun. Chișinău, str. N. Titulescu, 35	MD19TRPBAA317110D00792AC

Semnat:_____ Numele, Prenumele:_____ În calitate de: _____

Ofertantul: _____ Adresa:_____