Caiet de sarcini
la procedura de achiziţie a
licenţei antivirus prin contract de mică
valoare

1. **Denumirea autorităţii contractante:** **Administraţia Naţională a Penitenciarelor**
2. **IDNO:** ***1006601001012***
3. **Tip procedură achiziţie: Contract de mică valoare**
4. **Obiectul achiziţiei: Licenţă Antivirus**
5. **Cod CPV: 48700000-5**

Acest document este întocmit în scopul achiziţionării:

Licenţă Antivirus
[obiectul achiziţiei]

conform necesităţilor **Administraţiei Naţionale a Penitenciarelor**
[denumirea autorităţii contractante]

(în continuare – Cumpărător) pentru perioada bugetară 2021, este alocată suma necesară din:

Banca Ministerul Finanţelor – Trezoreria de Stat/ TREZMD2X
[sursa banilor publici]

6. **Cumpărătorul invită operatorii economici interesaţi, care îi pot satisface necesităţile să participe la procedura de achiziţie privind livrarea/prestarea următoarelor bunuri/servicii:**

Nr. d/o	Cod CPV	Denumirea serviciilor solicitate	Cantitatea	Specificaţia tehnică deplină solicitată
1.	48700000-5	**Licenţă Antivirus**	**200 bucăţi**	1. Se solicită prelungirea mentenanţei anuale a soluţiei corporative antivirus deja existente în cadrul instituţiei pentru o perioadă de 12 luni, pentru protecţia a 195 de staţii de lucru fizice şi virtualizate, 5 servere fizice. 2. Soluţia de securitate ofertată trebuie să se regăsească în Gartner în ultimii 3 ani de zile şi să ocupe locuri de top în testele internaţionale "AV-TEST" cel puţin 7 ani la rând. 3. Licenţele ofertate trebuie să fie capabile să prelungească pe un termen de 12 luni, licenţele existente compatibile sau echivalente pentru F-Secure EPP computers protection premium, server protection premium. *Termen de livrare:* 10 zile lucrătoare de la data intrării în vigoare a contractului, care include şi timpul lucrărilor de instalare, configurare şi punerea în funcţiune a soluţiei.

7. Documentele/cerinţele de calificare pentru operatorii economici includ următoarele:

	Denumirea documentului/cerinţei	Cerinţe suplimentare faţă de document	Obligativitatea
1	Oferta	Completat în conformitate cu anexa (pg. 6) în original, confirmat cu ştampila şi semnătura participantului sau semnat electronic;	Da
2	Certificat de atribuire al contului bancar	Eliberat de banca deţinătoare de cont, în original sau copie cu ştampilă şi semnătura participantului sau semnat electronic;	Da
3	Informaţii generale despre ofertant (sediul ofertantului şi al filialelor acestuia)	Format liber, cu ştampilă şi semnătura participantului sau semnat electronic;	Da
4	Dovada înregistrării juridice	Certificat/ decizie de înregistrare a întreprinderii/ extras din registrul de stat al persoanelor juridice,	Da

		emis de organul abilitat – copie, cu ştampila şi semnătura participantului sau semnat electronic	
5	Certificatului ISO 27001:2013 şi Certificatului ISO 9001:2015 al ofertantului	Copia - confirmată cu ştampilă şi semnătura participantului sau semnat electronic;	Da
6	Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul ofertat	Copia - confirmată cu ştampilă şi semnătura participantului sau semnat electronic;	Da
7	Autorizarea de la producător pentru licitaţia respectivă	Copia - confirmată cu ştampilă şi semnătura participantului sau semnat electronic;	Da
8	Certificat în calitate de auditor intern pentru sistemul de management al securităţii informaţionale conform ISO 27001:2013	Copia - confirmată cu ştampilă şi semnătura participantului sau semnat electronic;, pentru minim o persoană angajată a ofertantului;	Da
9	Minim 3 referinţe şi 3 recomandări de implementare pe piaţa locală a soluţiei ofertate.	Copia - confirmată cu ştampilă şi semnătura participantului sau semnat electronic;	Da
10	Minim 2 certificate tehnice pe soluţiile propuse.	Copia – confirmată cu ştampilă şi semnătura participantului sau semnat electronic;	Da
11.	*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, menţinerea funcţionalului soluţiei trebuie să fie executate de ofertant care trebuie sa facă parte din suportul local anual, iar costul acestora trebuie să fie incluse în oferta comercială.	Copia - confirmată cu ştampilă şi semnătura participantului sau semnat electronic;	Da

În situaţia identificării de către ANP a diferenţei între suma preţurilor unitare şi preţul total din ofertă, 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.*

8. Operatorii economici interesaţi pot obţine informaţie suplimentară sau pot solicita clarificări de la autoritatea contractantă prin intermediul platformei achiziţii.md

Denumirea autorităţii contractante: Administraţia Naţională a Penitenciarelor.

a) Adresa: municipiul Chişinău, str. N. Titulescu, 35

b) Tel: 409-830, 709-748.

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

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

1. Cerințele tehnice functionale minim solicitate față de soluția antivirus:

Soluția trebuie să asigure protecție și management centralizat pentru stații de lucru, servere și dispozitive mobile cu următoarele sisteme de operare:

Stații de lucru:

- Microsoft Windows 7 Service Pack 1; 8.1; 10; (all 32-bit and 64-bit editions);
- macOS 10.12, 10.13, 10.14;

Servere:

- Microsoft® Windows Server 2008 R2; 2012; 2012 Essentials; 2012 R2; 2012 R2 Essentials; 2012 R2 Foundation; 2016 Standard; 2016 Essentials; 2016 Datacenter; 2016 Core; 2019 Standard; 2019 Essentials; 2019 Datacenter; 2019 Core; CentOS, Debian, Oracle Linux, RHCK and UEK, RHEL, SUSE Linux Enterprise Server 11 SP3, SP4, Ubuntu, etc.

Dispozitive Mobile:

- Android 4.03 sau mai sus; iOS 9.x sau mai sus care să ofere browsing protection separat securizat, mobile VPN pentru protecția personală, protecție malware cel puțin pentru Android.
- 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 să asigure protecție în timp real, împotriva virușilor (ransomware – crypto) cu scopul prevenirii distrugerii și modificării datelor, amenințărilor spyware, rootkit-urilor, tentativelor de intruziune, spam-urilor și a altor mesaje nedorite.
- soluția trebuie să ofere actualizări automate a versiunilor noi si a hotfix-urilor;
- soluția trebuie să ofere protectie împotriva virușilor și noilor amenințări 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 și analiza vulnerabilităților din rețea;
- soluția trebuie să ofere funcționalități de firewall, intrusion prevention, application control si sanbox pentru analiza traficului de tip ransomware si detonarea acestuia;
- soluția trebuie să asigure criptarea automată prin VPN, a întregului trafic realizat dintre dispozitivele mobile, permițînd utilizarea în condiții de siguranță a Wi-Fi public și rețelelor mobile;
- soluția trebuie să ofere posibilități exacte de activare si 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 aplicare a politicilor pe mașini client, grupuri de mașini, domeniu, unități organizaționale sau utilizatori de Active Directory;
- soluția trebuie să ofere instalare centralizată a statiilor de lucru și terminalelor mobile;
- soluția trebuie să ofere consolă unică de management cu instalare în Cloud;
- 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 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 accesărilor 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 reputaţie); împiedicarea accesului la site-urile nepermise (Controlul conţinutului Web); blocarea accesului la tipurile de conţinut nepermise (Filtrare tipuri de conţinut).;

- soluţia trebuie să ofere funcţional de Controlul conexiunilor prin securizarea plăţilor online şi afişarea unui pop-up care blocheaza celelalte pagini şi imposibilitate accesării altor decît cea în care se efectueaza tranzacţia.
- soluţia trebuie să ofere funcţional de scanare în timp real a tuturor obiectelor pe care le accesează utilizatorii finali, pentru depistarea programelor de tip malware şi inclusiv să ofere posibilitatea de configurare şi efecuare a scanării manuale;
- soluţia trebuie să ofere funcţional de scanare a aplicaţiilor în cloud;
- soluţia trebuie să ofere funcţional de Scanare a semnăturilor;
- soluţia trebuie să includă funcţional de control a dispozitivelor externe, să ofere posibilitatea: de a seta restricţii în privinţa modului în care utilizatorii pot accesa dispozitive USB, precum dispozitive de stocare, camere USB şi imprimante; de a interzcie accesul la orice dispozitiv de stocare USB; de a stopa rularea executabilelor stocate pe astfel de dispozitive; de a seta restricţii pe grupuri de dispozitive;
- soluţia trebuie să ofere funcţional de analiză euristică si zero day, de comportament şi reputaţie;
- soluţia trebuie să ofere funcţional de Sandbox automatizat inclus – pentru analiza amănunţită prin detonarea fişierilor malitioase sau care nu pot fi protejate în baza de semnătură sau comportament;
- soluţia trebuie să ofere funcţional de control al aplicaţiilor, prin setarea unor reguli de blocare create ca excluderi pentru a bloca un acces anume şi să fie bazate:

• pe acţiuni precum permiterea, blocarea, sau permiterea şi monitorizarea aplicaţiilor;
• pe evenimente precum pornire aplicaţie, încărcare modul, pornire program de instalare, acces la fişiere, pornire aplicaţie şi încărcare modul;
• prin stabilirea unor condiţii care să poată fi selectate după atribute (cale destinaţie, nume fişier destinaţie, reputaţie destinaţie, versiune fişier destinaţie, cod hash pentru certificat la destinaţie, etc), condiţie şi valoare, ce vor asigura activarea regulilor de excludere;

- soluţia trebuie să ofere funcţional de Management API prin integrarea solutiilor terţe precum: SIEM/RMM;

2. Cerinţele tehnice vis-a-vis de administrarea soluţiei antivirus:

- administrarea soluţiei ofertate este necesară să se facă 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 funcţiona pe orice dispozitiv şi să conţină toate funţionalităţile sus solicitate;
- posibilitatea administrării centralizare, prin intermediul unei singure console, a urmatoarelor medii în cazul extinderii funcţionalului: staţii de lucru fizice şi virtualizate, servere fizice şi virtualizate, dispozitivelor mobile pe Android şi iOS, casuţelor poştale pe Exchange sau office 365, scanarea vulnerabilităţilor web şi a infrastructurii IT (interne si externe);
- să suporte următorele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari;
- interfaţa consolei de administare trebuie să asigure posibilitatea de funcţionare în limbile: romana, rusă şi engleză obligatoriu, cu capacitatea de a putea fi selectată limba dorită, în scopul unei administrări mai uşoare de către administratori;
- administratorul trebuie să poată permite sau interzice utilizatorului de a activa sau dezactiva caracteristicile de securitate setate;

3. Cerinţe vis-a-vis de funcţionalul de raportare şi alerte a solutiei antivirus:

- Soluţia 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 informaţie despre:
  - Clasament computere (după infecţii blocate);
  - Top de infecţii tratate;

- Infecţii gestionate;
- Starea de protecţie;
- Cele mai recente actualizări pentru definiţiile 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;
- Soluția trebuie să asigure posibilitatea de trimitere a alertelor in momentul declanșării prin email specificat de administrator și să permită setarea limbii dorite în care să fie emailul (minim română, engleză, rusă);
- 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.

11. Termenii și condițiile de livrare/prestare/executare solicitați: 10 zile lucrătoare de la data intrării în vigoare a contrcatului, care inlcude și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.

12. Termenul de valabilitate a contractului: 31.12.2021

13. Întocmirea ofertelor: ***Oferta (conform pag. 6) și documentele de calificare*** solicitate vor fi întocmite clar, fără corectări, cu număr și data de ieșire, cu semnătura persoanei responsabile și urmează a fi prezentate: Conform SIA RSAP Mtender, prin intermediul platformei achiziții.md; Ofertele întîrziate vor fi respinse.

14. Criteriul de atribuire este: prețul cel mai scăzut și corespunderea specificațiilor tehnice;

15. Tehnici și instrumente specifice de atribuire: licitație electronică în 3 runde cu pasul minim 1%

16. Termenul de valabilitate a ofertelor: ***60 de zile.***

17. Valoarea estimată a achiziției, fără TVA : 58 335,00 lei.

Conducătorul grupului de lucru: **Alexandru ADAM**

L.Ş.

Oferta

Numărul procedurii:	Data: 00.08.2021
Denumirea procedurii: **Licență Antivirus**	

Cod CPV	Denumirea bunurilor și/sau a serviciilor	Cantitatea	Preț unitar (fără TVA)	Preț unitar (cu TVA)	Suma fără TVA	Suma cu TVA	Specificația tehnică deplină propusă de ofertant	Termenul de livrare/ prestare
1	2	3	4	5	6	7	8	9
48700000-5	**Licență Antivirus**	200 bucăți						10 zile lucrătoare de la data intrări în vigoare a contractului, care inlcude ș timpul lucrărilor de instalare, configurare ș punerea în funcțiune a soluției.

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

Ofertantul: _____ Adresa: