Caiet de sarcini
la procedura de achiziție soluției de protecție si securitate antivirus pentru protectia infrastructurii prin contract de mică valoare

1. **Denumirea autorității contractante:Administrația Națională a Penitenciarelor**
2. **IDNO:** ***1006601001012***
3. **Tip procedură achiziție: Contract de mică valoare**
4. **Obiectul achiziției: Soluție corporativă antivirus de protecție și securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protectia a 195 de statii de lucru fizice/virtualizate) si 5 servere fizice/virtualizate.**
5. **Cod CPV: 48700000-5**

Acest document este întocmit în scopul achiziționării:
Soluție corporativă antivirus de protecție și securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protectia a 195 de statii de lucru fizice/virtualizate) si 5 servere fizice/virtualizate.
[obiectul achiziției]
conform necesităților Administrației Naționale a Penitenciarelor
[denumirea autorității contractante]
(în continuare – Cumpărător) pentru perioada bugetară 2020, este alocată suma necesară din: ***Banca Ministerul Finanțelor – Trezoreria de Stat/ TREZMD2X***
[sursa banilor publici]
Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile să participe la procedura de achiziție privind livrarea/prestarea următoarelor bunuri/servicii:

Nr. d/o	Cod CPV	Denumirea serviciilor solicitate	Cantitatea	Specificația tehnică deplină solicitată
1.		**Soluție corporativă antivirus de protecție și securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protectia a 195 de statii de lucru fizice/virtualizate) si 5 servere fizice/virtualizate.**	**200**	**I. Cerintele tehnice functionale minim solicitate:** - Soluție corporativă antivirus de protecție și securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protectia a 195 de statii de lucru fizice/virtualizate) si 5 servere fizice/virtualizate. - Solutia trebuie sa asigure protectie si management centralizat pentru statii de lucru, servere și dispozitive mobile cu urmatoarele 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 and later; iOS 9.x and later - 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 si analiza vulnerabilitatilor din retea; - 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, permițând 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 AD; - soluția trebuie să ofere instalare centralizată a statiilor de lucru si terminalelor mobile; - soluția trebuie să ofere consolă unică de management cu instalare in 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 actiuni (blocarea sau permiterea) și direcție(intrare sau iesire) pentru controlul și monitorizarea traficului la nivel de endpoint și rețea, care sa 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. - 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 aplicatiilor in cloud; - soluția trebuie să ofere funcțional de Scanare a semnăturilor; - 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 dispozitive USB, precum dispozitive de stocare, camere USB și 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 şi să fie bazate:

- pe actiuni 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 terte precum: SIEM/RMM;

II. Cerintele tehnice vis-a-vis de administrarea solutiei:

- administrarea soluţiei 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 funcţiona pe orice dispozitiv şi să conţină toate funţionalităţile sus solicitate;
- 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 si 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;

III. Cerinţe vis-a-vis de funcţionalul de raportare şi alerte:

-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;

- Soluţia trebuie să permită setarea şi configurarea de alerte, declanşarea lor să poată fi aplicată pentru minim următoarele

acţiuni: blocat, redenumit, oprit, şters, plasat, raportat, dezinfectat, în carantină, raportat către utilizator, blocat şi acţiune suplimentară solicitată de la utilizator, mutat în coşul de gunoi;

- Soluţia trebuie să asigure posibilitatea de trimitere a alertelor in momentul declanşării prin email spevificat de administrator si sa permită setarea limbii dorite in care să fie emailul (minim română, engleză, rusă);

IV. Alte cerinţe obligatorii:

- Pentru soluţia ofertată se solicită a fi 12 luni suport local şi de la producător.
- Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanţă, inclusiv suport local din partea partenerului.
- 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.
- Ofertantul va avea minim o persoana certificata in calitate de auditor intern pentru sistemul de management al securităţii informaţionale conform ISO 27001:2013;
- Solutia trebuie sa se regaseasca in Gartner in ultimii 3 ani de zile si sa ocupe locuri de top in testele internationale "AV-TEST".

Documentele/cerinţele de calificare pentru operatorii economici includ următoarele:

	Denumirea documentului/cerinţei	Cerinţe suplimentare faţă de document	Obligativitatea
1	Oferta	Autentificat cu semnătura Participantului;	Da
2	Certificat de atribuire al contului bancar		
3	Informaţii generale despre ofertant		
4	Dovada înregistrării juridice		
5	Prezentarea a minim 2 certificate tehnice pe solutia propusa.		
6	Certificatul ISO 27001:2013 (pe numele ofertantului)		
7	Certificatul ISO 9001:2015 (pe numele ofertantului)		
8	Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul ofertat.		
9	3 referinţe de implementare pe piaţa locală a soluţiei ofertate.		

2. **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.

3. **În cazul în care contractul este împărţit pe loturi un operator economic poate depune oferta (se va selecta):** Pentru toate loturile;
4. **Admiterea sau interzicerea ofertelor alternative:** nu se admite
5. **Termenii şi condiţiile de livrare/prestare/executare solicitaţi:** 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.
6. **Termenul de valabilitate a contractului:** 31.12.2020
7. **Întocmirea ofertelor**: ***Oferta (conform pag. 5) şi documentele de calificare*** solicitate vor fi întocmite clar, fără corectări, cu număr şi data de ieşire, cu semnătura persoanei responsabile şi urmează a fi prezentate:
   - pînă la: ora 08:00
   - pe: data 03.08.2020
   - prin intermediul platformei achiziţii.md
   - **Ofertele întîrziate vor fi respinse.**
8. **Criteriul de atribuire este:** *preţul cel mai scăzut*
9. **Termenul de valabilitate a ofertelor:** ***30 de zile.***
10. **Valoarea estimată a achiziţiei, fără TVA : 54 200,00 lei.**

Conducătorul grupului de lucru: **Alexandru ADAM**

L.Ş.

Oferta

Numărul procedurii: | Data: 03.08.2020

Denumirea procedurii: **Soluție corporativă antivirus de protecție și securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protectia a 195 de statii de lucru fizice/virtualizate) si 5 servere fizice/virtualizate**

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
[illegible]	Soluție corporativă antivirus de protecție și securitate in varianta Cloud, pentru o perioadă de 12 luni pentru protectia a 195 de statii de lucru fizice/virtualizate) si 5 servere fizice/virtualizate	200						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.

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

Ofertantul: _____ Adresa: