Formularul ofertei (F3.1)

[Ofertantul va completa acest formular în conformitate cu instrucţiunile de mai jos. Nu se vor permite modificări în formatul formularului, precum şi nu se vor accepta înlocuiri în textul acestuia.]
Data depunerii ofertei: "14" noiembrie 2019
Procedura de achiziţie Nr.: _____
Anunţ de participare Nr.: ID : ocds-b3wdp1-MD-1573126535189 din 07 noiembrie 2019
Către: **Inspectoratul National de Probatiune**
[numele deplin al autorităţii contractante]

SC Xontech Systems SRL declară că:
[denumirea ofertantului]

a) Au fost examinate şi nu există rezervări faţă de documentele de atribuire, inclusiv modificările nr._____.
[introduceţi numărul şi data fiecărei modificări, dacă au avut loc]

b) **SC Xontech Systems SRL** se angajează să
[denumirea ofertantului]

furnizeze/presteze, în conformitate cu documentele de atribuire şi condiţiile stipulate în specificaţiile tehnice şi preţ, următoarele bunuri
Pachete software de protecţie antivirus
[introduceţi o descriere succintă a bunurilor]

c) Suma totală a ofertei fără TVA constituie:

Lot 1- 41,900.00 (*patruzeci și unu mii noua sute Lei și zero bani, MDL).*

[introduceți prețul pe loturi (unde e cazul) și totalul ofertei în cuvinte și cifre, indicând toate sumele și valutele respective]

d) Suma totală a ofertei cu TVA constituie:

Lot 1 – 50,250.00 (*cinzeci de mii două sute cinzeci lei si zero bani, MDL).*

[introduceţi preţul pe loturi (unde e cazul) şi totalul ofertei în cuvinte şi cifre, indicînd toate sumele şi valutele respective]

e) Prezenta ofertă va rămîne valabilă pentru perioada de timp specificată în **FDA3.8.**, începînd cu data-limită pentru depunerea ofertei, în conformitate cu **FDA4.2.**, va rămîne obligatorie şi va putea fi acceptată în orice moment pînă la expirarea acestei perioade;
f) În cazul acceptării prezentei oferte, **SC Xontech Systems SRL**
[denumirea ofertantului]

se angajează să obţină o Garanţie de bună execuţie în conformitate cu **FDA7**, pentru executarea corespunzătoare a contractului de achiziţie publică.
g) Nu sîntem în nici un conflict de interese, în conformitate cu punctul**,** în conformitate cu art.74 din Legea nr.131 din 03.07.2015 privind achiziţiile publice.
h) Compania semnatară, afiliaţii sau sucursalele sale, inclusiv fiecare partener sau subcontractor ce fac parte din contract, nu au fost declarate neeligibile în baza prevederilor legislaţiei în vigoare sau a regulamentelor cu incidenţă în domeniul achiziţiilor publice.

Semnat:_____
[semnătura persoanei autorizate pentru semnarea ofertei]

Nume: **Irina Vicol**
În calitate de: **Administrator**
[funcţia oficială a persoanei ce semnează formularul ofertei]
Ofertantul: **SC Xontech Systems SRL**
Adresa: str. Alexandru cel bun 85, MD-2012, mun. Chisinau, Republica Moldova.
Data: "14" noiembrie 2019

Irina Vicol
Date: 2019.11.14 11:17:57 EET
Reason: MoldSign Signature
Location: Moldova

Specificații de preț (F4.2)

[Acest tabel va fi completat de către ofertant în coloanele 5,6,7,8, iar de către autoritatea contractantă – în coloanele 1,2,3,4,9,10]

	Numărul procedurii de achiziție ocds-b3wdp1-MD-1573126535189 din 07.11.19
	Denumirea procedurii de achiziție: Pachete software de protecţie antivirus

Cod CPV	**Denumirea bunurilor/serviciilor**	**Unitatea de măsură**	**Canti-tatea**	**Preţ unitar (fără TVA)**	**Preţ unitar (cu TVA)**	**Suma fără TVA**	**Suma cu TVA**	**Termenul de Livrare/prestare**	**Clasificație bugetară (IBAN)**
1	2	3	4	5	6	7	8	9	10
	Bunuri/servicii								
	Lotul 1								
48760000-3	Pachet software de protecţie antivirus pentru computere	bucăți	250	167,60	201.12	41,900.00	50,250.00	Livrarea în decurs de 10 zile, după înregistrarea contractului la trezorărie	MD83TRPBAA317110A00837AC
	TOTAL					**41,900.00**	**50,250.00**		

Semnat:_____
Numele, Prenumele: Irina Vicol
În calitate de: Administrator
Ofertantul:SC Xontech Systems SRL
Adresa: str. Alexandru cel bun 85, MD-2012, mun Chisinau, Republica Moldova

Specificaţii tehnice (F4.1)

[Acest tabel va fi completat de către ofertant în coloanele 3, 4, 5, 7, iar de către autoritatea contractantă în coloanele 1, 2, 6, 8]

	Numărul procedurii de achiziție ocds-b3wdp1-MD-1573126535189 din 07.11.19
	Denumirea procedurii de achiziție: Pachete software de protecţie antivirus

Cod CPV	Denumirea bunurilor/serviciilor	Modelul articolului	Ţara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7	8
	Bunuri						
48760000-3	Pachet software de protecţie antivirus pentru computere	Bitdefender Gravity Zone Business Security	Romania	Bitdefender	**Soluție antivirus** Se solicita o soluție de securitate centralizata 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 250 stații de lucru. Soluția furnizată trebuie: • Să conțină o consola de management cu o baza de date inclusa care sa fie non-relațională, 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. • 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	Produsul ofertat este „Bitdefender Gravity Zone Business Security” cu suport 12 luni. Produsul ofertat acopera toate cerintile cerute. Ofertantul va executa instalarea /configurarea si punerea in execuție a produsului pentru 10 stații de lucru din aparatul central. De asemenea va instrui administratorul IT din cadrul instituției privind exploatarea produsului.	-

					pentru sistemul de operare. Imaginea de tip „template” se va putea importa in: - *VMware vSphere* - *Citrix XenServer* - *Microsoft Hyper-V* - *Red Hat Enterprise Virtualization* - *KVM* - *Oracle VM.* • 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. • 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). • 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. • Soluția trebuie sa aibă posibilitatea integrării cu Active Directory 2003 si 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 in limba romana, adițional limba engleza si altele. • Interfața clientului de securitate, care se instalează pe stații si servere la fel va fi in limba romana, adițional limba engleza si altele. • Ofertantul va acorda manual de instalare si de administrare a produsului in limba romana. **1) Cerințe minime obligatorii pentru componenta de securitate dedicata stațiilor de lucru :** Soluția va permite creșterea pe aceeași licența un		

					număr nelimitat de dispozitive. Soluția va include: ● scanare automată a fișierelor, a memoriei și a cheilor de regiștri Windows înainte de instalarea pe sisteme. ● Soluția va 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. ● 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 automata in timp real va putea fi setata sa nu scaneze arhive sau fișiere mai mari de „ 100 ” 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 va permite aplicarea politicilor pe mașini client, grupuri de masini, domeniu, unitati organizationale.		

					• 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. • Vaccinul anti-ransomware primește actualizări de la producător, o dată cu actualizarea semnăturilor produsului Antimalware. Politica sa poate fi schimbata automat in funcție 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 virusi. • 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 în rețea. ● Soluția trebuie sa poată scana următoarele tipuri minime de sisteme: - Procesor compatibil Intel® Pentium 1,6 MHz, Memorie RAM: 1 GB - Sistem de operare, baze de date si browsere web: - Windows 7, 8.1, 10. ● 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 deținute. ● 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. **2) Operatorul economic va asigura următoarele servicii:** - Actualizarea bazei de semnături de virus si a motoarelor de scanare pe perioada de 12 luni. - In cazul in care in perioada de 12 luni de licențiere apare o versiune noua a produsului, producătorul va pune la dispoziție versiunea nouă gratuit. - Distribuirea unor mesaje de atenționare de urgență prin e-mail in cazul apariției unor noi viruși distructivi		

					sau cu potențial de răspândire rapida, - 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. - 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 executa instalarea /configurarea si punerea in execuție a produsului pentru 250 de stații de lucru in aparatul central cele 42 de subdiviziuni din teritoriu. De asemenea va instrui administratorul IT din cadrul instituției privind exploatarea produsului.		
	TOTAL						

Semnat:_____
Numele, Prenumele: Irina Vicol
În calitate de: Administrator
Ofertantul: SC Xontech Systems SRL
Adresa: str. Alexandru cel bun 85, MD-2012, mun Chisinau, Republica Moldova