APROB
Directorul Inspectoratului Național de Probațiune

Andrei IAVORSCHI

ANUNȚ DE PARTICIPARE

privind achiziționarea Pachete software de protecție antivirus ,
(se indică obiectul achiziției)
prin procedura de achiziție Achiziții cu costuri mici ,
(tipul procedurii de achiziție)

1. **Denumirea autorității contractante:** Inspectoratul Național de Probațiune ,
2. **IDNO:** 1010601000287 ,
3. **Adresa:** mun. Chișinău, str. V. Alecsandri, 1 ,
4. **Numărul de telefon/fax:** 022280995 / 022280905 / 022280978 ,
5. **Adresa de e-mail și de internet a autorității contractante:** logistica@probatiune.gov.md; www.probatiune.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):** Instituție 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	Unitatea de măsură	Cantitatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată (se va indica pentru fiecare lot în parte)
		Lotul 1				
1	48760000-3	Pachet software de protecție antivirus pentru computere	buc	250	**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 licenţa suplimentara 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.* • Soluţia va fi scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe maşini virtuale sau pe aceeaşi maşina virtuala. • Soluţia va include adiţional si un modul de balansare (load balancer) pentru cazurile in care mai multe maşini virtuale ale componentei de management sunt instalate cu acelaşi rol (pentru Load Balancing si performanta/redundanta). • Soluţia va include un mecanism de configurare a disponibilităţii pentru serverul cu baze de date (clustering pentru redundanta). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe maşini virtuale. • Soluţia trebuie sa aibă posibilitatea integrării cu Active Directory 2003 si versiuni mai recente. • Să ofere administratorilor de reţea posibilitatea identificării rapide a incidentelor legate de prezenţa unor programe periculoase şi să poată aplica diverse politici de securitate. • Interfaţa consolei de management va fi obligatoriu in limba romana, adiţional limba engleza si altele. • Interfaţa clientului de securitate, care se instalează pe staţii si servere la fel va fi in limba romana, adiţional limba engleza si altele. • Ofertantul va acorda manual de instalare si de administrare a produsului in limba romana. **1) Cerinţe minime obligatorii pentru componenta de securitate dedicata staţiilor de lucru :** Soluţia va permite creşterea pe aceeaşi licenţa un număr nelimitat de dispozitive. Soluţia va include: • scanare automată a fişierelor, a memoriei şi a cheilor de regiştri Windows înainte de instalarea pe sisteme. • Soluţia va permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate staţiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau staţiile critice. Astfel, serverul de actualizare trebuie sa includă actualizări de tip: ciclu rapid si ciclu lent. • Tehnologii de detectare, dezinfectare şi trimitere în carantină a virusilor, programelor spion de tip adware/spyware, troienilor şi 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 fişiere 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 desecuritate. • Configurarea, evaluarea, instalarea și îndepărtarea aplicațiilor la nivel desistem. 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.	
Valoarea estimativă totală Șef Direcția financiară, INP, Valeri Alexa _____ (semnătura)						42500,00

Specificația tehnică deplină elaborată de către Serviciul monitorizare electronica și tehnologii informaționale al INP, responsabil Valeriu Melinte, șef SMETI _____
(semnătura)

9. **În cazul în care contractul este împărțit pe loturi un operator economic poate depune oferta (se va selecta):**
   1) Pentru un singur lot;
   2) Pentru mai multe loturi;
   3) **Pentru toate loturile;**
   4) Alte limitări privind numărul de loturi care pot fi atribuite aceluiași ofertant _____.

10. **Admiterea sau interzicerea ofertelor alternative:** nu se admite
(indicați se admite sau nu se admite)

11. **Termenii și condițiile de livrare/prestare/executare solicitați:** Livrarea în decurs de 10 zile, după înregistrarea contractului la trezorărie.

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
(indicați da sau 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 se aplică
(se menționează respectivele acte cu putere de lege și acte administrative)

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 (DUAE, documentație):**

Nr. d/o	Descrierea criteriului/cerinței	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1	Oferta	Original, confirmat prin aplicarea ştampilei şi semnăturii Participantului.	Obligator
2	Specificații tehnice	Formularul F 4.1 Original, confirmat prin aplicarea ştampilei şi semnăturii Participantului.	Obligator
3	Specificații de preț	Formularul F 4.2 Original, confirmat prin aplicarea ştampilei şi semnăturii Participantului.	Obligator
4	Certificat/decizie de înregistrare a întreprinderii	Copie, confirmat prin aplicarea ştampilei şi semnăturii Participantului.	Obligator
5	Certificat cu privire la situația contribuabilului	Copia originalului eliberat de Inspectoratul Fiscal, confirmată prin aplicarea ştampilei şi semnăturii Participantului.	Obligator
6	Certificat privind deținerea contului bancar	Copia originalului, confirmat prin aplicarea ştampilei şi semnăturii Participantului.	Obligator
7	Declarație pe popria răspundere privind termenul de garanție	Declarație pe propria răspundere privind termenul de garanţie a Pachetului de software de protecţie antivirus pentru computere de minim 12 luni din data livrării. Original – confirmat prin semnătura şi ştampila Participantului	Obligator
8	Autorizarea de la producător pentru produsul propus.	Original, confirmat prin aplicarea ştampilei şi semnăturii Participantului.	Obligator
9	Certificatele ISO 9001 si 27001 de la producător pentru produsul propus.	Copia originalului, confirmat prin aplicarea ştampilei şi semnăturii Participantului.	Obligator

16. **Motivul recurgerii la procedura accelerată (în cazul licitației deschise, restrînse şi al procedurii negociate), după caz**: nu se aplică.

17. **Tehnici şi instrumente specifice de atribuire (dacă este cazul specificați dacă se va utiliza acordul-cadru, sistemul dinamic de achiziție sau licitația electronică):** Licitația electronică va fi în 3 runde, cu durata (conform Regulamentului SIA RSAP), pasul minim fiind 0,4-3% din valoarea estimată a lotului conform mențiunilor în SIA RSAP.

18. **Condiții speciale de care depinde îndeplinirea contractului** (indicați după caz): nu se aplică.

19. **Criteriul de evaluare aplicat pentru adjudecarea contractului:** cel mai mic preț.

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

Nr. d/o	Denumirea factorului de evaluare	Ponderea%

21. **Termenul limită de depunere/deschidere a ofertelor:**
    - **până la: conform mențiunilor** SIA RSAP.
    - **pe: conform mențiunilor** SIA RSAP.

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.

24. **Locul deschiderii ofertelor:** SIA RSAP.

(SIA RSAP sau adresa deschiderii)

Ofertele întîrziate 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 cînd 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 se aplică .
(se specifică denumirea proiectului și/sau programului)

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 se aplică .

30. **În cazul achizițiilor periodice, calendarul estimat pentru publicarea anunțurilor viitoare:** nu se aplică .

31. **Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț:** 12.09.2019 .

32. **Data transmiterii spre publicare a anunțului de participare:** SIA RSAP .

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	Se acceptă SIA RSAP
sistemul de comenzi electronice	Nu se acceptă
facturarea electronică	Se acceptă
plățile electronice	Se acceptă

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 .
(se specifică da sau nu)

35. **Alte informații relevante:** _____

Conducătorul grupului de lucru: Petru Vîrlan

L.Ș.

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 achiziţie _____din_____
	Denumirea procedurii de achiziţie: Achiziţii cu costuri mici

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				**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 pentru sistemul de operare. Imaginea de tip „template" se va putea importa in: - *VMware vSphere* - *Citrix XenServer* - *Microsoft Hyper-V*		0

					- *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 şi trimitere în carantină a virusilor, programelor spion de tip adware/spyware, troienilor şi 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 fişiere mai mari de „ 100 ” MB, mărimea fişierelor putând fi definita de administratorul soluţiei, 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 parţial scanarea locala. • Administratorul poate personaliza şi motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare, fie scanare locala sau scanare hybrida. • Soluţia oferă protecţie in timp real pe maşinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata. • Soluţia trebuie sa trimită în carantină fişierele suspecte sau infectate, în vederea reducerii riscului de propagare. Astfel administratorul va putea alege pentru fişiere infectate sau suspecte următoarele: interzice accesul, dezinfectează, ştergere, muta fişierele in carantina, nicio acţiune si alte acţiuni alternative. • Protecţie firewall individuală pentru utilizatorii de la distanţă şi ocazionali. • Risc redus de infectare prin scanarea în timp real a traficului internet a tuturor staţiilor de lucru. • Creşterea productivităţii şi a nivelului de securitate prin blocarea accesului utilizatorilor la anumite site-uri ori prin blocarea posibilităţii de a transmite email-uri conţinând date confidenţiale. • Colectarea de date despre ameninţările informatice actuale de la toate staţiile de lucru şi serverele din reţea cu ajutorul interfeţei panoului de control. • Management şi configurare de la distanţă, în conformitate cu politica desecuritate.		

					• Configurarea, evaluarea, instalarea şi îndepărtarea aplicaţiilor la nivel desistem. Niveluri multiple de protecţie avansată, soluţia 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 maşini client, grupuri de masini, domeniu, unitati organizationale. • Pentru o mai buna protecţie a staţiilor si serverelor, solutia trebuie sa includa un vaccin anti-ransomware. Acest vaccin va asigura protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea staţiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare. • Vaccinul anti-ransomware primeşte actualizări de la producător, o dată cu actualizarea semnăturilor produsului Antimalware. Politica sa poate fi schimbata automat in funcţie de: g) User-ul logat pe statie h) IP sau clasa de IP al statiei i) Gateway-ul alocat j) DNS serverul alocat k) Clientul este/nu este in aceeaşi reţea cu infrastructura de management l) Tipul reţelei (lan, wireless) • Actualizări automate a bazei de date ce conţine semnături de viruşi. • Soluţia 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:_____ În calitate de: _____

Ofertantul: _____ Adresa: _____

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_____din_____
	Denumirea procedurii de achiziție: Achiziții cu costuri mici

Cod CPV	Denumirea bunurilor/serviciilor	Unitatea de măsură	Canti-tatea	Preț unitar (fără TVA)	Preț 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					Livrarea în decurs de 10 zile, după înregistrarea contractului la trezorărie	MD83TRPBAA317110A00837AC
	TOTAL								

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

Ofertantul: _____ Adresa: _____