I.M. Orange Moldova S.A.
IDNO 1003600106115
Str. Alba Iulia 75, MD-2071 Chisinau
Republica Moldova
Capital social 179499609 lei
Administrator Olga Surugiu
www.orange.md

Anexa nr. 7
la Documentația standard
aprobată prin Ordinul Ministrului Finanțelor
nr. 115 din 15.09.2021

CERERE DE PARTICIPARE

Către: **Poșta Moldovei**,
mun.Chişinău, bd. Ștefan Cel Mare și Sfânt, nr. 134.

Stimați domni,

Ca urmare a anunțului de participare apărut în Buletinul achizițiilor publice, nr. **ocds-b3wdp1-MD-1784732374102 (21658469)** din 22.07.2026, privind aplicarea procedurii pentru atribuirea contractului **„Pachete software antivirus”**, noi **Î.M. „Orange Moldova” S.A.**, am luat cunoștință de condițiile și de cerințele expuse în documentația de atribuire și exprimăm prin prezenta interesul de a participa, în calitate de ofertant/candidat, neavând obiecții la documentația de atribuire.

Data completării 12.08.2026

Cu stimă,

Dana ARGINT
Director Vânzări Corporative și Soluții ICT
Î.M. „Orange Moldova” S.A.

Acest act este semnat prin aplicarea **Semnăturii Mobile**
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

I.M. Orange Moldova S.A.
IDNO 1003600106115
Str. Alba Iulia 75, MD-2071 Chisinau
Republica Moldova
Capital social 179499609 lei
Administrator Olga Surugiu
www.orange.md

Anexa nr. 8
la Documentația standard
aprobată prin Ordinul Ministrului Finanțelor
nr. 115 din 15.09.2021

DECLARAȚIE
privind valabilitatea ofertei

Către: **Poșta Moldovei**,
mun.Chişinău, bd. Ștefan Cel Mare și Sfânt, nr. 134.

Stimați domni,

Ne angajăm să menținem oferta valabilă, privind achiziționarea **„Pachete software antivirus”**, nr. **ocds-b3wdp1-MD-1784732374102 (21658469)** din **22.07.2026** prin procedura de achiziție **Licitație deschisă**, pentru o durată de **60 zile** (șaizeci zile), respectiv până la data de **12.10.2026**, și ea va rămâne obligatorie pentru noi și poate fi acceptată oricând înainte de expirarea perioadei de valabilitate.

Data completării 12.08.2026

Cu stimă,

Dana ARGINT
Director Vânzări Corporative și Soluții ICT
Î.M. „Orange Moldova” S.A.

Acest act este semnat prin aplicarea **Semnăturii Mobile**
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

Formularul ofertei pentru bunuri şi servicii

Data depunerii ofertei: **11.08.2026**

Procedura de achiziţie Nr.: **ocds-b3wdp1-MD-1784732374102**

Anunţ de participare Nr.: ***36 (treizeci şi şase)***

Către: ***Întreprinderea de Stat „Poşta Moldovei”***

Î.M. „Orange Moldova” S.A. **declară că:**

a) Au fost examinate şi nu există rezervări fată de documentele de atribuire, inclusiv modificările nr. -

(introduceţi numărul şi data fiecărei modificări, dacă au avut loc)

b) **Î.M. „Orange Moldova” S.A.** se angajează să presteze, în conformitate cu documentele de atribuire şi condiţiile stipulate în specificaţiile tehnice şi preţ, următoarele: ***Pachete software antivirus***

c) Suma totală a ofertei fără TVA constituie:

790,470.00 lei (şapte sute nouăzeci de mii patru sute şaptezeci lei, 00 bani)

d) Suma totală a ofertei cu TVA constituie:

948,564.00 lei (nouă sute patruzeci şi opt de mii cinci sute şaizeci şi patru lei, 00 bani)

e) Prezenta ofertă va rămâne valabilă pentru perioada de timp de ***60*** zile, începând cu data-limită pentru depunere a ofertei, în conformitate cu **Anexa nr. 22 „Specificaţia tehnică” şi Anexa nr. 23 „Specificaţia de preţ”**, astfel va rămâne obligatorie şi va putea fi acceptată în orice moment până la expirarea acestei perioade;

f) 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.

Data completării 12.08.2026

Dana ARGINT
Director Vânzări Corporative și Soluții ICT
Î.M. „Orange Moldova” S.A.

Acest act este semnat prin aplicarea **Semnăturii Mobile**

Verificarea semnăturii - https://msign.gov.md/#/verify/upload

I.M. Orange Moldova S.A.
IDNO 1003600106115
Str. Alba Iulia 75, MD-2071 Chisinau
Republica Moldova
Capital social 179499609 lei
Administrator Olga Surugiu
www.orange.md

Anexa nr. 23
la Documentația standard
aprobată prin Ordinul Ministrului Finanțelor
nr. 115 din 15.09.2021

Specificații de preț

Numărul procedurii de achiziție: *ocds-b3wdp1-MD-1784732374102 (21658469) din 22.07.2026*
Obiectul achiziției: *Pachete software antivirus*

Cod CPV	Denumirea bunurilor/ serviciilor	Unitatea de măsură	Canti-tatea	Preț unitar (fără TVA)	Preț unitar (cu TVA)	Suma totală fără TVA	Suma totală cu TVA	Termenul de livrare/ prestare	Clasificație bugetară (IBAN)
1	2	3	4	5	6	7	8	9	10
	Lotul nr. 1 - Pachete software antivirus								
48200000-0	Pachete software antivirus (inclusiv Disk Encryption management)	buc.	1000	790.47	948.56	790,470.00	948,564.00	*Livrarea va fi efectuată prin canalele oficiale ale producătorului, în termen de până la 15 (cincisprezece) zile calendaristice din data semnării contractului*	MD36ML0000000 00225183434
	Total					790,470.00	948,564.00		

Data completării 12.08.2026
Dana ARGINT
Director Vânzări Corporative și Soluții ICT
Î.M. „Orange Moldova” S.A.

Acest act este semnat prin aplicarea **Semnăturii Mobile**
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

I.M. Orange Moldova S.A.
IDNO 1003600106115
Str. Alba Iulia 75, MD-2071 Chisinau
Republica Moldova
Capital social 179499609 lei
Administrator Olga Surugiu
www.orange.md

Anexa nr. 22
la Documentația standard
aprobată prin Ordinul Ministrului Finanțelor
nr.115 din 15.09.2021

Specificații tehnice

Numărul procedurii de achiziție: *ocds-b3wdp1-MD-1784732374102 (21658469) din 22.07.2026*

Obiectul achiziției: *Pachete software antivirus*

Denumirea serviciilor	Denumirea serviciilor	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Lotul nr. 1 - Pachete software antivirus						
Pachete software antivirus (inclusiv Disk Encryption management)	Kaspersky Next XDR Optimum	Elveția (Switzerland)	Kaspersky	Conform Anexei nr.1	Conform Anexei nr.1	n/a

Data completării 12.08.2026
Dana ARGINT
Director Vânzări Corporative și Soluții ICT
Î.M. „Orange Moldova” S.A.

Acest act este semnat prin aplicarea **Semnăturii Mobile**
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

I.M. Orange Moldova S.A.
IDNO 1003600106115
Str. Alba Iulia 75, MD-2071 Chisinau
Republica Moldova
Capital social 179499609 lei
Administrator Olga Surugiu
www.orange.md

Specificația tehnică

<table>
<tr><th>Specificarea tehnică deplină solicitată de către autoritatea contractantă</th><th>Specificarea tehnică deplină propusă de către ofertant</th></tr>
<tr><td colspan="2">Lotul nr. 1 – Pachete software antivirus</td></tr>
<tr><td>
<u>Tip</u>: Subscriere anuală pentru soluția de protecție și securitate pentru 1000 entități (PC/ laptop/ VDI/ Server) pentru perioada de 3 ani.
<u>Cantitate:</u> Ofertantului este responsabil de a determinarea modelului de licențiere luând în calcul:
• 1000 entități (PC/laptop/VDI/Server);
• Disk Encryption management pentru 1000 entități.

Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări ”AV-TEST”, ”VIRUS BULLETIN’S”, ”REAL-WORLD PROTECTION”, ”MALWARE PROTECTION”).

<u>Caracteristici generale ale produsului:</u>

Soluția trebuie să reprezinte o platformă integrată pentru managementul securității, gândită ca o soluție modulară.
Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management:
• Protecție stații și servere fizice și virtualizate;
• Serviciu de corelare și răspuns la evenimente de tip EDR (endpoint detection and response).

<u>Consola de management:</u>

Accesibilitate atât de pe browser desktop cât și tip mobile.
Să ofere opțiune configurabilă de actualizare automată a consolei de management.

<u>Soluția de scanare centralizată:</u>

Soluția trebuie să asigure protecția mediilor virtualizate (VDI), inclusiv a mediilor persistente și non-persistente, și să fie compatibilă cu următoarele platforme de virtualizare:
1. VMware vSphere;
2. Citrix XenServer;
3. Microsoft Hyper-V.
</td><td>
<table>
<tr><th>Product</th><th>Package</th><th>Qty</th><th>Term</th></tr>
<tr><td>Kaspersky Next XDR Optimum 1000</td><td>License</td><td>1000</td><td>3 year</td></tr>
</table>

<u>Tip</u>: Subscriere anuală pentru soluția de protecție și securitate pentru 1000 entități (PC/ laptop/ VDI/ Server) pentru perioada de 3 ani.
<u>Cantitate:</u>
• 1000 entități (PC/laptop/VDI/Server);
• Disk Encryption management pentru 1000 entități.

Produsul antivirus oferit ocupă locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări ”AV-TEST”, ”VIRUS BULLETIN’S”, ”REAL-WORLD PROTECTION”, ”MALWARE PROTECTION”).

<u>Caracteristici generale ale produsului:</u>

Soluția este o platformă integrată pentru managementul securității, gândită ca o soluție modulară.
Produsul conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management:
• Protecție stații și servere fizice și virtualizate;
• Serviciu de corelare și răspuns la evenimente de tip EDR (endpoint detection and response).

<u>Consola de management:</u>

Accesibilitate atât de pe browser desktop cât și tip mobile.
Oferă opțiune configurabilă de actualizare automată a consolei de management.

<u>Soluția de scanare centralizată:</u>

Soluția asigură protecția mediilor virtualizate (VDI), inclusiv a mediilor persistente și non-persistente, și să fie compatibilă cu următoarele platforme de virtualizare:
</td></tr>
</table>

I.M. Orange Moldova S.A.
IDNO 1003600106115
Str. Alba Iulia 75, MD-2071 Chisinau
Republica Moldova
Capital social 179499609 lei
Administrator Olga Surugiu
www.orange.md

Cerințe generale produs: Soluția trebuie să: • permită activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management; • ofere vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi si îmbunătățiri, probleme rezolvate, probleme cunoscute; • afișeze notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore *(configurabile)*: licențiere, detecție virusi, actualizări de produs disponibile. ***Panou de monitorizare si raportare (Dashboard):*** • să ofere posibilitatea creării rapoartelor configurabile după tip, țintă și scop cu opțiuni specifice pentru orice tip de raport cu posibilități de adăugare/eliminare și rearanjare. • să prezinte rapoarte pentru toate modulele suportate *(stare/statut/actualizare)*. ***Inventarierea rețelei – managementul securității:*** Produsul trebuie să: • se integreze cu domenii Active Directory multiple, să poată importa inventarul. • permită descoperirea PC neintegrate în Active Directory (Workgroup); • ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare si adresa IP, politica aplicată, online și/sau offline și FQDN; • permită instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale; • permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale; • permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus; • ofere posibilitatea de repornire a mașinilor fizice de la distanță; • ofere informații detaliate despre fiecare task inițiat și afișarea statutului lui; • permită configurarea centralizată a clienților antivirus prin intermediul politicilor; • ofere în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături; • permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea.	**4.** VMware vSphere; **5.** Citrix XenServer; **6.** Microsoft Hyper-V. ***Cerințe generale produs:*** Soluția: • permite activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management; • oferă vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi si îmbunătățiri, probleme rezolvate, probleme cunoscute; • afișează notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore *(configurabile)*: licențiere, detecție virusi, actualizări de produs disponibile. ***Panou de monitorizare si raportare (Dashboard):*** • oferă posibilitatea creării rapoartelor configurabile după tip, țintă și scop cu opțiuni specifice pentru orice tip de raport cu posibilități de adăugare/eliminare și rearanjare. • prezintă rapoarte pentru toate modulele suportate *(stare/statut/actualizare)*. ***Inventarierea rețelei – managementul securității:*** Produsul: • se integrează cu domenii Active Directory multiple, să poată importa inventarul. • permite descoperirea PC neintegrate în Active Directory (Workgroup); • ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare si adresa IP, politica aplicată, online și/sau offline și FQDN; • permite instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale; • permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale; • permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus; • oferă posibilitatea de repornire a mașinilor fizice de la distanță; • oferă informații detaliate despre fiecare task inițiat și afișarea statutului lui; • permită configurarea centralizată a clienților antivirus prin intermediul politicilor; • oferă în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături;

Politici: Produsul trebuie să: • permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module; • conțină opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user; • permită aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directoy; • poată fi schimbată automat în funcție de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în accesai rețea cu infrastructura de management, Tipul rețelei (lan, wireless). ***Monitorizare și raportare:*** Produsul trebuie să: • permită setarea de opțiuni specifice pentru afișarea rapoartelor existente; • dețină un panou central care să afișeze statutul modulelor și rapoartele lor pentru perioadele de timp specificate; • conțină rapoarte care prezinta statutul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate; • trimită rapoarte către un număr nelimitat de adrese de email; • permită vizualizarea rapoartelor curente programate de administrator; • permită exportarea rapoartelor în format .pdf si detaliile ca format .csv; • includă un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise si ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal; • ofere interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor; • ofere interogări legate de evenimente precum: calculatorul țința pe care a avut loc evenimentul, tipul starea și configurația agentului de securitate instalat, starea modulelor și rolurilor de protecție instalate pe agentul de securitate, denumirea și alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicații blocate, detecțiile etc);	• permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea. ***Politici:*** Produsul: • permite configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module; • conține opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user; • permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directoy; • poate fi schimbată automat în funcție de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în accesai rețea cu infrastructura de management, Tipul rețelei (lan, wireless). ***Monitorizare și raportare:*** Produsul: • permite setarea de opțiuni specifice pentru afișarea rapoartelor existente; • deține un panou central care să afișeze statutul modulelor și rapoartele lor pentru perioadele de timp specificate; • conține rapoarte care prezinta statutul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate; • trimite rapoarte către un număr nelimitat de adrese de email; • permite vizualizarea rapoartelor curente programate de administrator; • permite exportarea rapoartelor în format .pdf si detaliile ca format .csv; • include un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise si ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal; • oferă interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor; • oferă interogări legate de evenimente precum: calculatorul țința pe care a avut loc evenimentul, tipul starea și configurația agentului de securitate instalat, starea modulelor și rolurilor de protecție instalate pe agentul de securitate, denumirea și alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicații blocate, detecțiile etc);

I.M. Orange Moldova S.A.
IDNO 1003600106115
Str. Alba Iulia 75, MD-2071 Chisinau
Republica Moldova
Capital social 179499609 lei
Administrator Olga Surugiu
www.orange.md

Carantină: • Produsul trebuie să permită restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă; • Administrarea Carantinei să fie posibilă atât pe terminalul administrat cât și din consola de management; ***Utilizatori:*** • Administrarea este necesar să fie efectuată pe bază de roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter și alte roluri configurabile detaliat cu posibilitatea de selectare a serviciilor și obiectelor pentru care un utilizator poate face modificări; • Utilizatorii să poată fi importați din Microsoft Active Directory sau creați în consola de management; • Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp - configurabil. ***Log-uri:*** • Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare. ***Actualizare:*** Soluția va permite: • Definirea de locații de actualizare multiple; • Activarea/dezactivarea actualizărilor; • Testarea noilor versiuni înainte de a fi instalate pe toți clienții *(posibilitate de actualizare în mai multe cicluri – 1 mediu de test, 2 – mediu de producție);* • Definirea zonelor de test și zonelor critice de producție. ***Protecție stații și servere fizice si virtualizate – caracteristici minime:*** Soluția trebuie să: • Permită instalarea personalizată a modulelor; • Includă un „vaccin” anti-ransomware, cu actualizări de la producător, pentru protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar daca sunt infectate și blocarea procesului de criptare; • Includă protecție împotriva atacurilor zero-day de tip exploit *(atacuri direcționate);*	***Carantină:*** • Produsul permite restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă; • Administrarea Carantinei posibilă atât pe terminalul administrat cât și din consola de management; ***Utilizatori:*** • Administrarea este efectuată pe bază de roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter și alte roluri configurabile detaliat cu posibilitatea de selectare a serviciilor și obiectelor pentru care un utilizator poate face modificări; • Utilizatorii pot fi importați din Microsoft Active Directory sau creați în consola de management; • Posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp - configurabil. ***Log-uri:*** • Soluția permite înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare. ***Actualizare:*** Soluția permite: • Definirea de locații de actualizare multiple; • Activarea/dezactivarea actualizărilor; • Testarea noilor versiuni înainte de a fi instalate pe toți clienții *(posibilitate de actualizare în mai multe cicluri – 1 mediu de test, 2 – mediu de producție);* • Definirea zonelor de test și zonelor critice de producție. ***Protecție stații și servere fizice si virtualizate – caracteristici minime:*** Soluția: • Permite instalarea personalizată a modulelor; • Include un „vaccin” anti-ransomware, cu actualizări de la producător, pentru protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar daca sunt infectate și blocarea procesului de criptare; • Include protecție împotriva atacurilor zero-day de tip exploit *(atacuri direcționate);*

• Includă modul de analiză la risc capabil să identifice și să remedieze riscurile identificate la nivel de rețea sau sistem de operare, cu posibilitate de configurare și automatizare; • Includă un modul avansat de securitate bazat pe tehnologii de machine learning, analiză comportamentală și algoritmi euristici, proiectat pentru detectarea atacurilor avansate și a activităților suspecte înainte de faza de execuție; • Includă modul avansat de securitate pentru protecție împotriva: atacurilor direcționate *(Targeted Attack),* fișierelor suspecte si traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecărui tip de amenințare trebuie să i se poată configura independent nivelul de protecție și acțiunile aplicate, în funcție de capabilitățile soluției ofertate și recomandările producătorului; • Includă modul de sandbox, unde se vor putea trimite manual sau automat fișiere pentru a putea fi „detonate" pentru o analiză în profunzime; • Includă variante de analiză a sandbox-ului tip: doar monitorizare sau blocare cu acțiuni de remediere: implicită și de siguranța. Pentru acțiunea implicită: doar raportare, dezinfecție, ștergere și transmitere în carantină. Pentru acțiunea de siguranța: ștergere sau permutare în carantină; • Suporte "detonarea" în modulul sandbox, minim, tipurile de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML *(Unicode)*, JAR *(archive),* JS, LNK, MHTML *(doc),* MHTML *(ppt),* MHTML *(xls),* Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files *(executable),* PDF, PEF *(executable),* PIF *(executable),* RTF, SCR, URL *(binary),* VBE, VBS, WSF, WSH, WSH-VBS, XHTML. Acestea vor fi detectate corect chiar dacă vor fi în arhive de tipul : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP *(multivolume),* ZOO, XZ ; • Ofere posibilitate de filtrare a incidentelor din interfața grafică în funcție intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac, sistem de operare afectat cît și după IP, nume fișier, nume stație; • Permită vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod: să generează o hartă de principiu a incidentului, să detalieze incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, să poată genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigare – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod); • Poată bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;	• Include modul de analiză la risc capabil să identifice și să remedieze riscurile identificate la nivel de rețea sau sistem de operare, cu posibilitate de configurare și automatizare; • Include un modul avansat de securitate bazat pe tehnologii de machine learning, analiză comportamentală și algoritmi euristici, proiectat pentru detectarea atacurilor avansate și a activităților suspecte înainte de faza de execuție; • Include modul avansat de securitate pentru protecție împotriva: atacurilor direcționate *(Targeted Attack),* fișierelor suspecte si traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecărui tip de amenințare trebuie să i se poată configura independent nivelul de protecție și acțiunile aplicate, în funcție de capabilitățile soluției ofertate și recomandările producătorului; • Include modul de sandbox, unde se vor putea trimite manual sau automat fișiere pentru a putea fi „detonate" pentru o analiză în profunzime; • Include variante de analiză a sandbox-ului tip: doar monitorizare sau blocare cu acțiuni de remediere: implicită și de siguranța. Pentru acțiunea implicită: doar raportare, dezinfecție, ștergere și transmitere în carantină. Pentru acțiunea de siguranța: ștergere sau permutare în carantină; • Suportă "detonarea" în modulul sandbox, minim, tipurile de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML *(Unicode)*, JAR *(archive),* JS, LNK, MHTML *(doc),* MHTML *(ppt),* MHTML *(xls),* Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files *(executable),* PDF, PEF *(executable),* PIF *(executable),* RTF, SCR, URL *(binary),* VBE, VBS, WSF, WSH, WSH-VBS, XHTML. Acestea vor fi detectate corect chiar dacă vor fi în arhive de tipul : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP *(multivolume),* ZOO, XZ ; • Oferă posibilitate de filtrare a incidentelor din interfața grafică în funcție intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac, sistem de operare afectat cît și după IP, nume fișier, nume stație; • Permite vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod: să generează o hartă de principiu a incidentului, să detalieze incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, să poată genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigare – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod); • Poate bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;

• Poată excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere malițioase într-o listă neagră pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase; • Permită deschiderea unei conexiuni remote către un endpoint potențial infectat pentru a permite o investigare rapidă a gazdei/ colectare date despre atacul respectiv/ remediere în timp real a breșelor de securitate/ permită executarea unor comenzi în linia de comandă care se execută cu privilegii de kernel pentru eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare; • Permită crearea regulilor de detecție customizabilă bazată pe procese, fișiere, registre și conexiuni de rețea; • Permită creare regulilor de excludere customizabilă bazată pe procese, fișiere, registre si conexiuni de rețea; • Permită căutarea pro activă pe endpoint-urile protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registre, valori de registre; • Permită deschiderea unei conexiuni remote către un endpoint potențial infectat pentru investigare rapidă, colectare date și remedierea în timp real a breșei de securitate, reducând timpul de remediere (downtime) în cazul unui atac, executarea comenzilor în linia de comandă cu privilegii de kernel ce permit eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare; • Includă modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response") capabil să identifice amenințări avansate sau atacuri în curs de desfășurare. Acest modul va fi capabil să:	• Poate excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere malițioase într-o listă neagră pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase; • Permite deschiderea unei conexiuni remote către un endpoint potențial infectat pentru a permite o investigare rapidă a gazdei/ colectare date despre atacul respectiv/ remediere în timp real a breșelor de securitate/ permită executarea unor comenzi în linia de comandă care se execută cu privilegii de kernel pentru eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare; • Permite crearea regulilor de detecție customizabilă bazată pe procese, fișiere, registre și conexiuni de rețea; • Permite creare regulilor de excludere customizabilă bazată pe procese, fișiere, registre si conexiuni de rețea; • Permite căutarea pro activă pe endpoint-urile protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registre, valori de registre; • Permite deschiderea unei conexiuni remote către un endpoint potențial infectat pentru investigare rapidă, colectare date și remedierea în timp real a breșei de securitate, reducând timpul de remediere (downtime) în cazul unui atac, executarea comenzilor în linia de comandă cu privilegii de kernel ce permit eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare; • Include modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response") capabil să identifice amenințări avansate sau atacuri în curs de desfășurare. Acest modul va fi capabil să:
a) *cuprindă colectarea de date și evenimente despre hardware și software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o hartă detaliata a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate;* ***b)*** *ofere senzori de colectare a datelor și componente de procesare și interpretare a acestora;* ***c)*** *posede capacitarăți de evaluare a activității tipice a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") și va raporta orice deviație de la acest comportament sub forma unui incident;* ***d)*** *ofere vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat generînd o hartă de principiu a incidentului, detaliind incidentul în funcție de amprenta de timp a fiecărei actiuni aferente incidentului, respectiv butonul „acționează" care poate genera un set de masuri specifice fiecărui element din harta incidentului (kill,*	***h)*** *cuprinde colectarea de date și evenimente despre hardware și software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o hartă detaliata a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate;* ***i)*** *oferă senzori de colectare a datelor și componente de procesare și interpretare a acestora;* ***j)*** *posedă capacitarăți de evaluare a activității tipice a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") și va raporta orice deviație de la acest comportament sub forma unui incident;* ***k)*** *oferă vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat generînd o hartă de principiu a incidentului, detaliind incidentul în funcție de amprenta de timp a fiecărei actiuni aferente incidentului, respectiv butonul „acționează" care poate genera un set de masuri specifice fiecărui element din harta incidentului (kill,*

carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod); ***e)*** *poate bloca fișiere si/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;* ***f)*** *poată excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere malițioase într-o listă pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase;* ***g)*** *permită vizualizarea incidentelor extinse corelate de pe mai multe endpoint-uri.* ***Cerințe de sistem:*** • Sisteme de operare pentru stații de lucru: Windows 7/10/11 (inclusiv Embebed și IoT), Mac OS X de la 10.12 și mai recent, Red Hat Enterprise Linux / CentOS 7 și mai recent, Oracle Linux 6.3 și mai recent, Ubuntu 16 și mai recent, SUSE Linux Enterprise Server 12 și mai recent, OpenSUSE 15 și mai recent, Fedora 31 și mai recent; • Sisteme de operare Windows pentru servere: Windows Server 2012/2012 R2/2016/2019/2022. ***Administrare și instalare remote:*** • Pachetele de instalare trebuie să fie configurabile cu modulele necesare cu domenii tip firewall, device control, power user, content control, disk encryption, EDR sensor, „relay” *(update server”);* • Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management; • Din consola să fie disponibile informații despre fiecare endpoint: numele, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări; • Posibilități de creare kit pentru endpoint – tip: universar – 32/64bit, fizic/VDI, web installe/full; • Gestionare, creare și configurare grupuri pentru endpoint ce nu sunt în AD; • Posibilitate de atribuire a funcționalității de descoperire a endpointurilor și în afara AD, pentru oricare endpoint. ***Caracteristici și funcționalități principale ale modulului antivirus:*** Produsul trebuie sa permită: • Stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni:	*carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod);* ***l)*** *poate bloca fișiere si/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;* ***m)*** *poate excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere malițioase într-o listă pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase;* ***n)*** *permite vizualizarea incidentelor extinse corelate de pe mai multe endpoint-uri.* ***Cerințe de sistem:*** • Sisteme de operare pentru stații de lucru: Windows 7/10/11 (inclusiv Embebed și IoT), Mac OS X de la 10.12 și mai recent, Red Hat Enterprise Linux / CentOS 7 și mai recent, Oracle Linux 6.3 și mai recent, Ubuntu 16 și mai recent, SUSE Linux Enterprise Server 12 și mai recent, OpenSUSE 15 și mai recent, Fedora 31 și mai recent; • Sisteme de operare Windows pentru servere: Windows Server 2012/2012 R2/2016/2019/2022. ***Administrare și instalare remote:*** • Pachetele de instalare trebuie să fie configurabile cu modulele necesare cu domenii tip firewall, device control, power user, content control, disk encryption, EDR sensor, „relay” *(update server”);* • Exista posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management; • Din consola este disponibilă informații despre fiecare endpoint: numele, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări; • Posibilitatea de creare kit pentru endpoint – tip: universar – 32/64bit, fizic/VDI, web installe/full; • Gestionare, creare și configurare grupuri pentru endpoint ce nu sunt în AD; • Posibilitate de atribuire a funcționalității de descoperire a endpointurilor și în afara AD, pentru oricare endpoint. ***Caracteristici și funcționalități principale ale modulului antivirus:*** Produsul permite: • Stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi. Astfel administratorul poate alege între următoarele acțiuni:

a) *implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune;* ***b)*** *alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină;* ***c)*** *acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune;* ***d)*** *acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină;* • Scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau fișiere mai mari de ” x” MB, definirea nivelelor de profunzime pentru scanarea în arhive; • Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă; • Scanarea oricărui suport de stocare a informației *(CD-uri, harduri externe, unități partajate etc);* • Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP; • Configurarea căilor ce urmează a fi scanate la cerere; • Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware; • Setarea priorităților scanărilor programate; • Soluția trebuie să permită configurarea mecanismelor de scanare utilizând tehnologii locale, bazate pe cloud sau alte mecanisme echivalente oferite de producător, pentru optimizarea performanței și consumului de resurse; • Administratorul trebuie să poată configura politicile și mecanismele de scanare disponibile, inclusiv utilizarea tehnologiilor locale, bazate pe cloud sau a altor mecanisme echivalente, în funcție de infrastructura protejată și recomandările producătorului; • Setarea a tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor; • Scanarea paginilor web; • Setarea a unei parole pentru protecția la dezinstalare; • Modul de antiphishing;	***e)*** *implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune;* ***f)*** *alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină;* ***g)*** *acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune;* ***h)*** *acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină;* • Scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau fișiere mai mari de ” x” MB, definirea nivelelor de profunzime pentru scanarea în arhive; • Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă; • Scanarea oricărui suport de stocare a informației *(CD-uri, harduri externe, unități partajate etc);* • Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP; • Configurarea căilor ce urmează a fi scanate la cerere; • Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware; • Setarea priorităților scanărilor programate; • Soluția permite configurarea mecanismelor de scanare utilizând tehnologii locale, bazate pe cloud sau alte mecanisme echivalente oferite de producător, pentru optimizarea performanței și consumului de resurse; • Administratorul poate configura politicile și mecanismele de scanare disponibile, inclusiv utilizarea tehnologiilor locale, bazate pe cloud sau a altor mecanisme echivalente, în funcție de infrastructura protejată și recomandările producătorului; • Setarea a tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor; • Scanarea paginilor web; • Setarea a unei parole pentru protecția la dezinstalare; • Modul de antiphishing;

• Protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată; • Soluția trebuie să suporte implementarea în medii VDI persistente și non-persistente, inclusiv utilizarea imaginilor de referință *(Golden Image/Template)* sau a unor mecanisme echivalente oferite de producător; • Utilizarea uni modul adițional de securitate bazat pe algoritmi tunabili de machine learning respectiv algoritmi euristici agresivi capabili să detecteze și blocheze atacuri de tip persistent sau targetat precum și alte categorii de malware sofisticat înainte de faza de execuție. Acest modul oferă următoarele funcționalități: ***a)*** *clasificarea tipului de atac;* ***b)*** *abilitatea de a configura acțiunile aplicate amenințărilor detectate, inclusiv raportarea, monitorizarea sau blocarea acestora;* ***c)*** *abilitatea de a configura nivelul de sensibilitate al mecanismelor de detecție și politicilor de securitate, conform recomandărilor producătorului;* ***d)*** *abilitatea de a acționa în mod diferit în funcție de tipul amenințării (fișier sau atac prin rețea);* • Posibilitatea de restaurare a fișierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, cînd determină că procesul este malițios; • Oprirea atacurile avansate de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive; • Depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare; • Protejarea aplicațiilor utilizate frecvent și a celor de tip „sistem” cum ar fi browserele, aplicațiile de tip office sau reader, procesele critice aferente sistemelor de operare. ***Firewall:*** • Sa ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate; • Modulul să poată fi instalat/ activat/ dezactivat/ dezinstalat la cerere; • Să permită definirea de rețele de încredere pentru mașina destinație. ~~***Protecția datelor:***~~ ~~• Produsul trebuie să permite blocarea datelor confidențiale *(pin-ul cardului, cont bancar etc)* transmise prin HTTP sau SMTP prin crearea unor reguli specifice.*~~	• Protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată; • Soluția suportă implementarea în medii VDI persistente și non-persistente, inclusiv utilizarea imaginilor de referință *(Golden Image/Template)* sau a unor mecanisme echivalente oferite de producător; • Utilizarea uni modul adițional de securitate bazat pe algoritmi tunabili de machine learning respectiv algoritmi euristici agresivi capabili să detecteze și blocheze atacuri de tip persistent sau targetat precum și alte categorii de malware sofisticat înainte de faza de execuție. Acest modul oferă următoarele funcționalități: ***e)*** *clasificarea tipului de atac;* ***f)*** *abilitatea de a configura acțiunile aplicate amenințărilor detectate, inclusiv raportarea, monitorizarea sau blocarea acestora;* ***g)*** *abilitatea de a configura nivelul de sensibilitate al mecanismelor de detecție și politicilor de securitate, conform recomandărilor producătorului;* ***h)*** *abilitatea de a acționa în mod diferit în funcție de tipul amenințării (fișier sau atac prin rețea);* • Posibilitatea de restaurare a fișierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, cînd determină că procesul este malițios; • Oprirea atacurile avansate de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive; • Depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare; • Protejarea aplicațiilor utilizate frecvent și a celor de tip „sistem” cum ar fi browserele, aplicațiile de tip office sau reader, procesele critice aferente sistemelor de operare. ***Firewall:*** • Sa ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate; • Modulul să poată fi instalat/ activat/ dezactivat/ dezinstalat la cerere; • Să permită definirea de rețele de încredere pentru mașina destinație. ~~***Protecția datelor:***~~ ~~• Produsul trebuie să permite blocarea datelor confidențiale *(pin-ul cardului, cont bancar etc)* transmise prin HTTP sau SMTP prin crearea unor reguli specifice.*~~

Nota*: Cerință eliminată în conformitate cu răspunsurile Autorității Contractante din 05.08.2026 și 06.08.2026, publicate în secțiunea „Clarificări” a procedurii de achiziție https://achizitii.md/ro/public/tender/21658469/questions.	**Nota*:** Cerință eliminată în conformitate cu răspunsurile Autorității Contractante din 05.08.2026 și 06.08.2026, publicate în secțiunea „Clarificări” a procedurii de achiziție https://achizitii.md/ro/public/tender/21658469/questions.
Controlul conținutului:	***Controlul conținutului:***
Produsul trebuie să ofere un modul integrat dedicat controlului accesului la Internet cu următoarele particularități: blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conțin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicații definite de administrator, restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite *(ex: online dating, violenta, pornografie etc).*	Produsul oferă un modul integrat dedicat controlului accesului la Internet cu următoarele particularități: blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conțin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicații definite de administrator, restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite *(ex: online dating, violenta, pornografie etc).*
Controlul dispozitivelor:	***Controlul dispozitivelor:***
Produsul trebuie să conțină un modul pentru controlul dispozitivelor care: • Poate fi instalat/dezinstalat conform setărilor stabilite; • Permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security Policies 153, IEEE 1284.4, IEEE 1394, Imaging Devices, Modems, Tape Drives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internal and External Storage; • Permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client; • Permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.	Produsul conține un modul pentru controlul dispozitivelor care: • Poate fi instalat/dezinstalat conform setărilor stabilite; • Permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security Policies 153, IEEE 1284.4, IEEE 1394, Imaging Devices, Modems, Tape Drives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internal and External Storage; • Permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client; • Permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.
Power User:	***Power User:***
Produsul trebuie să conțină un modul pentru setări specifice – power user care să: • Poată fi instalat/dezinstalat în funcție de preferința administratorului; • Permită posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa și modifica setările clientului antivirus dintr-o consola disponibilă local pe mașina client; • Permită administratorului soluției să suprascrie din consola setările aplicate de utilizatorii Power User.	Produsul conține un modul pentru setări specifice – power user care să: • Poate fi instalat/dezinstalat în funcție de preferința administratorului; • Permite posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa și modifica setările clientului antivirus dintr-o consola disponibilă local pe mașina client; • Permite administratorului soluției să suprascrie din consola setările aplicate de utilizatorii Power User.
Actualizare:	***Actualizare:***
Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor:	Produsul oferă posibilitatea de efectuare a actualizărilor:

• La nivel de stație în mod silențios *(fără avertizări);* • Folosind unul sau mai multe servere de actualizare; • Pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare. • Gestionabil – doar local sau și servere online.	• La nivel de stație în mod silențios *(fără avertizări);* • Folosind unul sau mai multe servere de actualizare; • Pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare. • Gestionabil – doar local sau și servere online.
Protecție Anti-Tampering:	***Protecție Anti-Tampering:***
• Va permite detecția driverelor vulnerabile pe dispozitivele conectate *(endpointuri)* și când sunt efectuate încercări avansate de atac pentru a dezactiva agentul de securitate, ceea ce poate duce la compromiterea integrității produsului; • Va permite detectarea de drivere vulnerabile pe dispozitivele conectate care pot fi exploatate de atacatori, reprezentând amenințări la adresa integrității produsului. Tehnologia este compatibilă cu sistemele de operare Windows și Linux; • Va fi capabilă să protejeze împotriva amenințărilor noi sau erorilor umane neintenționate ce ar putea fi proiectate pentru a permite acces neautorizat la kernel, ducând la compromiterea integrității poate detecta când funcțiile de tip callback ale agentului de securitate au fost eliminate sau dezactivate în mod malițios.	• Permite detecția driverelor vulnerabile pe dispozitivele conectate *(endpointuri)* și când sunt efectuate încercări avansate de atac pentru a dezactiva agentul de securitate, ceea ce poate duce la compromiterea integrității produsului; • Permite detectarea de drivere vulnerabile pe dispozitivele conectate care pot fi exploatate de atacatori, reprezentând amenințări la adresa integrității produsului. Tehnologia este compatibilă cu sistemele de operare Windows și Linux; • Capabil să protejeze împotriva amenințărilor noi sau erorilor umane neintenționate ce ar putea fi proiectate pentru a permite acces neautorizat la kernel, ducând la compromiterea integrității poate detecta când funcțiile de tip callback ale agentului de securitate au fost eliminate sau dezactivate în mod malițios.
Disk Encryption:	***Disk Encryption:***
Soluție pentru managementul criptării discurilor pentru 1000 entități. Soluția va oferi următoarele funcționalități minime: • Administrarea produsului trebuie să fie realizată din aceeași consolă de management ca și soluția de protecție antivirus; • Produsul va utiliza mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows și FileVault pentru Mac OSX; • Va asigura vizibilitatea completă asupra stării de criptare a dispozitivelor inclusiv: numele stației, IP-ul stației, sistemul de operare, ID-ul volumului/partiției, numele partiției, starea criptării partiției, tipul partiției: boot, non-boot, mărimea partiției în GB, ID-ul cheii de recuperare; • Produsul trebuie să asigure criptarea pentru Următoarele OS: Windows 7/10/11 Pro/Enterprise *(with TPM)*; WindowsServer 2012/2012 R2, 2016, 2019, 2022 *(with TPM)*, OSX de la 10.12.	Soluție pentru managementul criptării discurilor pentru 1000 entități. Soluția oferă următoarele funcționalități minime: • Administrarea produsului este realizată din aceeași consolă de management ca și soluția de protecție antivirus; • Produsul utilizeaza mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows și FileVault pentru Mac OSX; • Asigura vizibilitatea completă asupra stării de criptare a dispozitivelor inclusiv: numele stației, IP-ul stației, sistemul de operare, ID-ul volumului/partiției, numele partiției, starea criptării partiției, tipul partiției: boot, non-boot, mărimea partiției în GB, ID-ul cheii de recuperare; • Produsul asigură criptarea pentru Următoarele OS: Windows 7/10/11 Pro/Enterprise *(with TPM)*; WindowsServer 2012/2012 R2, 2016, 2019, 2022 *(with TPM)*, OSX de la 10.12.
Alte cerințe:	**Alte cerințe:**
Perioada de suport și menținere de la producător:	Perioada de suport și menținere de la producător:

1. Pentru soluția ofertată se solicită a fi 36 luni; **2.** Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță. ***Notă:*** *Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă.*	**3.** Pentru soluția ofertată este de 36 luni; **4.** Producătorul oferă suport 24/24, prin e-mail sau conectare de la distanță. ***Notă:*** *Lucrările de instalare, configurare, punerea în funcțiune a soluției vor fi executate de Î.M. „Orange Moldova" S.A., iar costul acestora sunt incluse în ofertă.*

Data completării 12.08.2026
Dana ARGINT
Director Vânzări Corporative și Soluții ICT
Î.M. „Orange Moldova" S.A.

Acest act este semnat prin aplicarea **Semnăturii Mobile**
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

Anexa nr. 3

Denumirea operatorului economic: **Î.M. „Orange Moldova" S.A.**
Titlul achiziției: ***Pachetelor software antivirus***
Nr. procedurii de achiziție: *ocds-b3wdp1-MD-1784732374102 (21658469)*

DECLARAȚIE
pe proprie răspundere privind îndeplinirea criteriilor de calificare și selecție

Subsemnatul(a), **Dana ARGINT** reprezentantul legal al **Î.M. „Orange Moldova" S.A.** în calitate de ofertant, la achiziția **Pachete software antivirus** organizată de către **Î.S. „Poșta Moldovei"**, declar pe propria răspundere, sub sancțiunea excluderii din procedura de achiziție și a sancțiunilor aplicate faptei de fals în acte publice, că în conformitate cu situațiile prevăzute la:

1. Art. 67, alin. (3) și (4) al Legii nr. 74 din 2020 privind achizițiile în sectoarele energeticii, apei, transporturilor și serviciilor poștale:

1.1. În ultimii 5 ani, nu am fost condamnați, prin hotărâre definitivă a unei instanțe judecătorești, pentru participare la activități ale unei organizații sau grupări criminale, pentru corupție, pentru fraudă și/sau pentru spălare de bani, pentru infracțiuni de terorism sau infracțiuni legate de activități teroriste, pentru finanțarea terorismului, exploatarea prin muncă a copiilor și pentru alte forme de trafic de persoane.

1.2. Nicio persoană ce este membru al organismului de administrare, de conducere sau de control al respectivului ofertant/candidat sau are putere de reprezentare, de decizie sau de control în cadrul acestuia nu a fost condamnată printr-o hotărâre definitivă a unei instanțe de judecată pentru infracțiunile prevăzute la **pct. 1.1.**;

2. Art. 68 al Legii, alin. (1) nr. 74 din 2020 privind achizițiile în sectoarele energeticii, apei, transporturilor și serviciilor poștale:

2.1. Nu ne aflăm în oricare dintre situațiile prevăzute la art. 19 al Legii 131 din 2015 privind achizițiile publice:

2.1.1. În ultimii 5 ani, nu am fost condamnați, prin hotărârea definitivă a unei instanțe judecătorești, pentru participare la activități ale unei organizații sau grupări criminale, pentru corupție, pentru fraudă și/sau pentru spălare de bani, pentru infracțiuni de terorism sau infracțiuni legate de activități teroriste, finanțarea terorismului, exploatarea prin muncă a copiilor și alte forme de trafic de persoane;

2.1.2. Nicio persoană ce este membru al organismului de administrare, de conducere sau de control al respectivului ofertant/candidat sau are putere de reprezentare, de decizie sau de control în cadrul acestuia nu a fost condamnată printr-o hotărâre definitivă a unei instanțe de judecată pentru infracțiunile prevăzute la **pct. 2.1.1.**;

2.1.3. Nu ne aflăm în proces de insolvabilitate ca urmare a hotărârii judecătorești;

2.1.4. Ne-am îndeplinit obligațiile de plată a impozitelor, taxelor și contribuțiilor de asigurări sociale în conformitate cu prevederile legale în vigoare în Republica Moldova sau în țara în care suntem stabiliți;

2.1.5. Nu am fost condamnați, în ultimii 3 ani, prin hotărârea definitivă a unei instanțe judecătorești, pentru o faptă care a adus atingere eticii profesionale sau pentru comiterea unei greșeli în materie profesională;

2.1.6. Nu am prezentat / nu prezentăm informații false sau am prezentat / prezentăm informațiile solicitate de către autoritatea contractantă în scopul demonstrării îndeplinirii criteriilor de calificare și selecție;

2.1.7. Nu am încălcat obligațiile aplicabile în domeniul mediului, muncii și asigurărilor sociale;

2.1.8. Nu ne facem vinovați de o abatere profesională, care ne pune la îndoială integritatea;

2.1.9. Nu am încheiat cu alţi operatori economici acorduri care vizează denaturarea concurenţei;

2.1.10. Nu ne aflăm într-o situaţie de conflict de interese care nu poate fi remediată în mod efectiv prin măsurile prevăzute la art. 79 al legii nr. 131 din 2015 privind achiziţiile publice;

2.1.11. Nu suntem incluşi în Lista de interdicţie a operatorilor economici;

2.1.12. Respectăm regimul de compatibilităţi prevăzut la art. 16 alin. (6) al legii nr. 131 din 2015 privind achiziţiile publice *„Persoanele fizice şi juridice care sunt înregistrate, au reşedinţa sau desfăşoară activitatea economică principală în jurisdicţii ori regiuni autonome ce nu implementează standarde internaţionale de transparenţă, precum şi persoanele juridice în componenţa cărora figurează, direct sau indirect, una sau mai multe persoane (fondatori, asociaţi, acţionari, administratori, beneficiari efectivi) care sunt înregistrate, au reşedinţa sau desfăşoară activitatea economică principală în astfel de jurisdicţii ori regiuni autonome. Metodologia de stabilire a jurisdicţiilor care nu implementează standarde internaţionale de transparenţă, precum şi lista jurisdicţiilor respective, în sensul prezentei legi, se aprobă de către Guvern, la propunerea Serviciului Prevenirea şi Combaterea Spălării Banilor, după consultarea Băncii Naţionale a Moldovei şi a Comisiei Naţionale a Pieţei Financiare.”.*

3. Art. 70 alin. (1) lit. c) a Legii nr. 74 din 2020 privind achiziţiile în sectoarele energeticii, apei, transporturilor şi serviciilor poştale:

3.1. Îndeplinim criteriile de selecţie stabilite de entitatea contractantă în conformitate cu prevederile legii nr. 74 din 2020 privind achiziţiile în sectoarele energeticii, apei, transporturilor şi serviciilor poştale:

3.1.1. Suntem de acord cu termenul de plată propus de către **Î.S. „Poşta Moldovei”** de nu mai puţin de 30 de zile din data prezentării facturilor fiscale şi a actelor de predare-primire;

Data completării 12.08.2026

Dana ARGINT
Director Vânzări Corporative și Soluții ICT
Î.M. „Orange Moldova” S.A.

Acest act este semnat prin aplicarea Semnăturii Mobile
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

I.M. Orange Moldova S.A.
IDNO 1003600106115
Str. Alba Iulia 75, MD-2071 Chisinau
Republica Moldova
Capital social 179499609 lei
Administrator Olga Surugiu
www.orange.md

Informații generale despre ofertant

1. Denumirea Firmei – **Î.M. „Orange Moldova" S.A.**
1. Adresa Firmei - str. Alba Iulia 75, MD-2071, Chișinău, Moldova
2. Oficiul de înregistrare - str. Alba Iulia 75, MD-2071, Chișinău, Moldova
3. Codul fiscal / IDNO - 1003600106115
4. Telefon de contact – 022 977700; Ion COZMA 69198955
5. E-mail – corporate@orange.md ; ion.cozma@orange.com
6. Tipul Companiei - privat
7. Fondatorul Companiei şi ultimul Patron - Orange Participations S.A., Administrator – Olga Surugiu
8. Decizia de înregistrare: Certificat de înregistrare nr. 0067000 eliberat la 24.04.2007, Extras din registrul de stat al persoanelor juridice, eliberat de I.P. "Agenția Servicii Publice"
9. Domeniile principale de activitate: Telecomunicații
10. Experiență în domeniu - 28 ani
11. Licențe în domeniu:
    a) Seria AC Nr. 000229, 06.11.2014 – 06.11.2029, emis de ANRCETI. Genul de activitate - Utilizarea frecventei 2G, 1800 MHz
    b) Seria A MMI Nr. 004509, 09.12.2023 – 06.11.2029, emis de ANRCETI. Genul de activitate - Utilizarea frecventei 3G, 2100 MHz
    c) Seria AA Nr. 082488, 08.11.2012 – 08.11.2027, emis de ANRCETI. Genul de activitate - Utilizarea frecventei 4G, 2500 MHz
    d) Declaratie informativa Nr. C335539/2024, ANRCETI din 19.08.2024.
    e) Seria A MMI Nr.004587, 03.03.2025 – 03.03.2050, emis de ANRCETI. Genul de activitate - Utilizarea frecventei 5G, 1500 MHz
    f) Seria A MMI Nr.004586, 04.03.2025 – 03.03.2050, emis de ANRCETI. Genul de activitate - Utilizarea frecventei 5G, 3600 MHz
12. Denumirea Băncii la care Companiei are deschis cont bancar – BC „MAIB" S.A. suc. MAIB PARK, AGRNMD2X522, IBAN-MD64AG000000225110801767
13. Persoana împuternicită de a semna contractul, inclusiv datele procurii valabile (dacă este cazul) cu anexarea copiei: Dana Argint (procura nr. OMD 448 din 24.06.2025)
14. Declarăm disponibilitatea de semnare a contractului cu semnătura electronică:
15. ■ DA
16. □NU,deoarece _____

(se va include justificarea de ce nu se poate de semnat contractul cu semnătură electronică)

Data completării 12.08.2026

Dana ARGINT
Director Vânzări Corporative și Soluții ICT
Î.M. „Orange Moldova" S.A.

Acest act este semnat prin aplicarea **Semnăturii Mobile**
Verificarea semnăturii - https://msign.gov.md/#/verify/upload