"RTS ONE" S.R.L.
https://rts.md
(+373) 22 101 777
office@rts.one
str. Mitropolit G. Bănulescu-Bodoni 59/B, of. 815

Anexa nr. 22
la Documentația standard pentru procedura de achiziție, cu nr. de identificare în SIA RSAP Mtender: **ocds-b3wdp1-MD-1660717339009**

SPECIFICAȚII TEHNICE

Numărul procedurii de achiziție: MTender ID: **ocds-b3wdp1-MD-1660717339009**
Denumirea procedurii de achiziție: Achiziționarea, instalarea și configurarea pachetelor software antivirus în cadrul infrastructurii informatice a CNPF

Denumirea bunurilor	**Modelul articolului**	**Ţara de origine**	**Producă-torul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referinţă**
2	3	4		5	6	7
Achiziționarea, instalarea și configurarea pachetelor software antivirus în	Bitdefender GravityZone Business Security Premium (Elite)	Romania	Romania	Conform anexei nr.1 – Termeni de referință	Produsul este o platformă de management al securității endpoin-urilor, gândită ca o soluție modulară și scalabilă, bazată pe tehnologia atât Cloud cât și On-Premise, pentru a minimiza resursele locale. Licențele oferite sunt capabile să prelungească pe un termen de 12 luni, licențele existente compatibile sau echivalente pentru Bitdefender GravityZone Business Security Premium (Elite)	

cadrul infrastructurii informatice CNPF					**CONSOLA DE MANAGEMENT** **1. Cerinte generale:** 1.1. Consola de management și baza de date este inclusă fără a fi nevoie de softuri și licențe adiționale. 1.2. Interfața consolei de management este atât în limba română cât și engleză. 1.3. Interfața clientului de securitate se instalează pe statiți și servere. va fi in limba română sau engleză. 1.4. Solutia include un modul de update server prin care se asigură actualizarea de produs și a semnăturilor. 1 .5. Notificări - Soluția permite setarea și configurarea de alerte, declanșarea lor, poate fi aplicată pentru următoarele acțiuni: blocat, redenumit, oprit, sters, plasat, raportat, dezinfectat, în carantină, raportat către utilizator, blocat și acțiune suplimentară solicitată de la utilizator, mutat în coșul de gunoi și ulterior expediata către o cutie poștală sau mai multe. 1.6. Soluția permite integrarea cu un server Syslog ori SIEM pentru raportarea evenimentelor. 1.7. Soluția permite crearea unei copii de siguranță a profilului de configurație. **2. Panou de monitorizare și raportare (Dashboard):** 2.1. Rapoartele poate fi configurată specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport. 2.2. Rapoartele din panoul central de comanda permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea. **3. Inventarierea rețelei — managementul securității:** 3.1. Soluția permite descoperirea mașinilor din Microsoft Hyper-V. 3.2. Soluția permite descoperirea stațiilor fără protecție în Active Directory. 3.3. Soluția oferă opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP. 3.4. Soluția permite instalarea la distanță sau manual a clienților anti-malware pe mașini fizice/virtuale. 3.5. Soluția permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale. 3.6. Soluția permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalare de la distanță pentru endpoint-uri. 3.7. Soluția oferă posibilitatea de repornire a mașinilor fizice de la distanță.	

					3.8. Soluția oferă informații detaliate despre fiecare task și va afișa dacă task-ul s-a linalizat cu succes sau nu. 3.9. Soluția permite configurarea centralizată a clienților anti-malware prin intermediul politicilor. 3.10. Se oferă în consola de management informații detaliate ale obiectelor din consolă: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizări, Versiunea produsului, Versiunea de semnături. 3.11. Soluția permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea. **4. Politici:** 4.1. Soluția permite configurarea setarilor clientului anti-malware prin intermediul politicilor ce cont in setări pentru toate modulele. 4.2. Politica conține opțiuni specifice de activare/dezactivare și configurarea functionalităților precum scanarea anti-malware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user. **5. Rapoarte:** 5.1. Soluția conține rapoarte care prezintă starea endpoint-urilor din punct de vedere a1 actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate. 5.2. Soluția permite vizualizarea rapoartelor curente programate de administrator. 5.3. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, mentinând informațiile concise și ordonate corespunzător. 5.4. Interogarea legată de starea terminalului include informatii precum: 5.4.1. tip endpoint; 5.4.2. intrastructura retelei căreia îi aparține endpointul; 5.4.3. datele agentului de securitate; 5.4.4. starea modulelor de protecție; 5.5. Interogarea legată de evenimente endpoint include informații precum: 5.5.1. endpoint-ul pe care a avut loc evenimentul; 5.5.2. tipul starea și configurația agentului de securitate instalat; 5.5.3. starea modulelor și rolurilor de protecție instalate pe agentul de securitate; 5.5.4. denumirea și alocarea politicii; 5.5.5. utilizatorul autentificat în timpul evenimentului; 5.5.6. evenimente (site-uri blocate, aplicații blocate, detecțiile etc);	

					5.5.7. Soluția permite generarea de rapoarte grafice detaliate, cu posibilitate de export în format (docx, xml, xlsx), inclusiv cu remitere către adrese de email speciticate. Posibilitatea de a configura o frecvență pentru crearea rapoartelor după (zi, săptămăna, luna, ora), rapoartele cuprind minim informație despre: *5.5.7.1. Vulnerabilitățile descoperite care sunt clasificate după severitate: informativ, severitate minimă, severitate medie, și severitate înaltă;* *5.5.7.2. Notarea severității vulnerabilităților se face pe o notă de la 1 la 10;* *5.5.7.3. Raportul descrie fiecare vulnerabilitate în parte cu unele referințe;* *5.5.7.4. Recomandările propuse pentru remedierea vulnerabilitătii depistate;* *5.5.7.5. Crearea unei statistici grafice în dependență de vulnerabilitățile depistate;* *5.5.7.6. Top vulnerabilități depistate.* 5.5.8. Soluția permite crearea unor widgeturi care pot fi editate, clonate sau șterse cu afisarea lor pe pagină în mod dinamic. La fel, widgeturi de bord pot fi create în forma minim de: tabel, diagramă circulară (placintă), histograma, etc. 5.5.9. Tablourile de bord conțin informații ca: vulnerabilitățile depistate care vor fi grupate după severitate/dată/lună/cantitatea depistată. Cele mai grave vulnerabilități. Scanările active, scanările care sunt planiticate, ultimele dispozitive scanate. 5.5.10. Soluția permite setarea și configurarea de alerte. declanșarea lor poată fi aplicată pentru minim următoarele acțiuni: când pornește un proces de scanare, finalizarea procesului de scanare, la crearea și asignarea unui task către un utilizator existent. **6. Carantină:** 6.1. Soluția permite restaurarea fișierelor din carantină în locația originala. 6.2. Carantina va fi locală, pe fiecare stație administrată și va fi administrată, fie local, fie din consola de management. **7. Utilizatori:** 7.1. Administrarea se va putea face pe baza de roluri predefinite (Administrator, Auditor) sau roluri personalizate. 7.2. Administrator companie: administrează arhitectura consolei de management și serviciile de securitate; 7.3. Auditor: monitorizează și generează rapoarte. 7.4. Utilizatorii pot fi creați în consola de management.	

					7.5. Permite configurarea detaliată a drepturilor administrative, permitând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări. **8. Log-uri:** 8.1. Înregistrarea acțiunilor utilizatorilor. 8.2. Oferă informații detaliate pentru fiecare acțiune a unui utilizator. 8.3. Permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune. **9. Actualizare:** 9.1. Permite definirea de locații de actualizare multiple. 9.2. Permite activarea/dezactivarea actualizărilor de produs și semnături. 9.3. Permite actualizarea produsului într-o rețea fără acces la Internet. 9.4. Orice client antivirus poata fi configurat să livreze update-urile către alt client antivirus. 9.5. Soluția dispune de un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat din Cloud, fără intervenția administratorului. Astfel, administratorul va putea descarca pachetele pentru protecția stațiilor și serverelor pe care ruleaza sistemul de operare Windows, Linux, poate descărca pachetele pentru modul de scanare centralizată în mediile de virtualizare Hyper-V. 9.6. În cadrul serverului de actualizare, pentru o mai buna urmarire a actualizărilor pachetele pentru protecția statiilor și serverelor sau a pachetelor pentru modul de scanare centralizata, se va putea vizualiza un jurnal de modificări în care sunt precizate istoric: 9.6.1. versiunea pachetului; 9.6.2. data versiunii; 9.6.3. functii not si lmbun ătă tiri; 9.6.4. probleme rezolvate; 9.6.5. probleme cunoscute. 9.7. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului anti-malware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau statiile critice. Astfel, serverul de actualizare include 2 tipuri de actualizări de produs: 9.8. Ciclu rapid, gândit pentru un mediu de test în cadrul re{e1ei 9.9. Ciclu lent, gândit pentru restul rețelei (productie, servere critice etc) 9.10. Solutia permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management.	

					9.11. Soluția oferă posibilitatea de actualizare a aplicatiților învechite instalate pe stațiile de lucru. **10. Certificate:** 10.1. Accesul la consola de management se face doar prin HTTPS. 10.2. Soluția permite afișarea în consola de management informații despre certificate: nume, autoritatea emitentă, data eliberării și data expirării certiticatelor eliberate. **PROTECȚIE STAȚII ȘI SERVERE FIZICE/VIRTUALE** **11. Caracteristici generale:** 11.1. Pentru reducerea la minim a consumului de resurse, solutia anti-malware trebuie permite instalarea personalizată a modulelor deținute (de exemplu, sa permită instalarea soluției anti-malware fără modulul de control al accesului web, modul de control a1 dispozitivelor sau modulul firewall). 11.2. Pentru o mai buna protectie a statiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigură protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare. 11.3. Vaccinul anti-ransomware primește actualizări de la producător, odata cu actualizarea semnăturilor produsului Anti-malware. 11.4. Pentru o mai buna protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate). **12. Cerințe de sistem:** 12.1 . Sisteme de operare pentru statii de lucru pe 32/64 biti: Windows 11, Windows 10. 12.2. Sisteme de operare pentru servere: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012. 12.3. Terminale Servere: Microsoft Windows Terminal/RDP Services. 12.4. Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 7.3 sau mai recent, Ubuntu 16.04 LTS sau mai recent, SUSE Linux Enterprise Server 12 sau mai recent, Oracle Linux 7 sau mai recent, Debian 9 sau mai recent. **13. Administrare și instalare de la distanță:**	

					13 1 . Înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulate dorite: firewall, browsing protection, device control, software update, application control, network location settings, automated tasks, dataguard (sandbox). 13.2. Instalarea poate face în mai multe moduri: 13.2.1. prin descărcarea directa a pachetului pe statia pe care se va face instalarea; 13.2.2. prin instalarea la distanta, direct din consola de management. 13.3. Instalarea clientilor la distanta in alte locati i decat cele in care este instalata consola de management pentru a minimiza traficul in WAN. 13.4. In consola sunt disponibile informații despre fiecare stație: numele statiei, IP, sistem de operare. module instalate, politica aplicata, informații despre actualizări etc. 13.5. Din consola se poate trimite o singura politica pentru contigurarea integrala a clientului de pe statii/servere. 13.6. Consola va include o sectiune, „Audit", unde se vor menționa toate acțiunile intreprinse în politica de securitate cu informații detaliate: logare, editare, creare etc. **14. Caracteristici și functionalități principale ale modulului anti-malware:** 14.1. Soluția permite administratorului să stabilească acțiunea luată de produsul Anti-malware la detectarea unei amenințări noi. Astfel, administratorul poate alege între urmatoarele acțiuni: 14.1.1. Acțiune implicită pentru fișiere infectate: *14.1.1.1. interzice accesul;* *14.1.1.2. dezinfectează;* *14.1.1.3. ștergere;* *14.1.1.4. mută fișierele în carantină;* *14.1.1.5. nicio acțiune;* 14.1.2. Acțiune alternativă pentru fișierele infectate: *14.1.2.1. interzice accesul ;* *14.1.2.2. dezinfectează:* *14.1.2.3. ștergere;* *14.1.2.4. mută fișierele în carantină.* 14.1.3. Acțiune implicită pentru fișierele suspecte: *14.1.3.1. interzice accesul;* *14.1.3.2. ștergere;* *14.1.3.3. mută fișierele în carantină;* *14.1.3.4. nicio acțiune;* 14.1.4. Acțiune alternativă pentru fișierele suspecte: *14.1.4.1. interzice accesul;* *14.1.4.2. ștergere;*	

					14.1.4.3. mută fișierele în carantină. 14.2. Scanarea automată in timp real poate fi setată să nu scaneze arhive. 14.3. Scanarea euristică comportamentală prin simularea unui calculator virtual in interiorul căruia sunt rulate aplicatii cu potential periculos protejand sistemul de virusi necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă. 14.4. Scanarea oricărui suport de stocare a informatiei (CD-uri, harduri exteme, unități partajate etc). 14.5. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP. 14.6. Configurarea cailor ce urmează a fi scanate la cerere. 14.7. Clienții anti-malware pentru stațiile de lucru sa permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese. 14.8. Cu ajutorul unei baze de date complete cu semnături de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware. 14.9. Posibilitatea de configura scanările programate să se execute cu prioritate redusa. 14.10. Pentru o protectie sporitii, solutia anti-malware trebuie să aibă 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișiere1or și bazată pe monitorizarea proceselor. 14.11. Pentru o protecție sporită, soluția anti-malware trebuie să poata scana paginile HTTP. 14.1 2. Pentru o mai bună gestionare a anti-malware instalat pe stații, produsul va include opțiunea de setare a unei parole pentru protectia la dezinstalare. 14.13. Pentru siguranța utilizatorului, clientul va include un modul de anti-phishing. 14.14. Soluția oferă protectie în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată. **15. Firewall:** 15.1. Posibilitatea de configurarea regulilor de firewall pentru aplicații sau conectivitate. 15.2. Modulul poate fi instalat/dezinstalat în funcție de preferinta administratorului. 15.3. Posibilitatea de a defini rețele de incredere pentru masina destinatie.	

					16. Carantină: 16.1. Produsul anti-malware să permită trimiterea automata a fișierelor din carantină către laboratoarele anti-malware ale producătorului. 16.2. Trimiterea conținutului carantinei va putea fi expediat în mod automat, la un interval definit de administrator. 16.3. Produsul anti-malware să permită ștergerea automată a fișierelor din carantină mai vechi de o anumita perioadă, pentru a nu incărca inutil spațiul de stocare. **17. Protecția datelor:** 17.1. Produsul permite blocarea datelor confidentiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. **18. Controlul conținutului:** 18.1. Consola are integrat un modul dedicat controlului accesului la Internet în următoarele particularități: 18.1.1. Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini. 18.1.2. Permite controlul accesului numai la anumite pagini de Internet specificate de administrator; 18.1.3. Permite blocarea accesului la anumite aplicații definite de administrator; 18.1.4. Permite restricționarea accesului pe anumite pagini de Internet după anumite categorii prestabilite (ex: online dating, violenta. pomografie etc). **19. Controlul aplicațiilor:** 19.1. Pentru prevenirea infectării stațiilor și serverelor dar și pentru a permite aplicațiilor descoperite în rețea să se poată actualiza, solutia permite definirea unor programe de actualizare (Updater) care vor și lăsate sa actualizeze diferite aplicații instalate pe stații sau servere. 19.2. Soluția include opțiunea de a permite sau a bloca rularea anumitor aplicatii sau procese definite de administrator (inclusiv sub procese) după: 19.2.1. Target path; 19.2.2. Target SHA1 ; 19.2.3. Target SHA256; 19.2.4. Target file size; 19.2.5. Target signer name: 19.2.6. Target certificate hash; 19.2.7. Target has trusted signature;	

					19.2.8. Parent path; 19.2.9. Parent signer name; 19.2.10. Parent certificate hash; 19.2.11. Parent has trusted signature. **20. Controlul dispozitivelor:** 20.1. Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului. 20.2. Modulul va permite controlul următoarelor tipuri de dispozitive: 20.2.1. USB Mass Storage Device; 20.2.2. Wireless devices; 20.2.3. DVD/SC-ROM drivers; 20.2.4. Windows CE ActiveS ync devices; 20.2.5. Floppy drivers; 20.2.6. Modems; 20.2.7. COM & LTP ports; 20.2.8. Printers; 20.2.9. Smart Card Readers; 20.2.10. Imaging Device (cameras and scanners) 20.2.11. IEEE 1394 Host Bus Controllers 20.2.12. IrDA Devices 20.2.13. Bluestooth Devices 20.3. Modulul permite configurarea de reguli prin care se definesc permisiunile pentru dispozitivele conectate la mașina client. 20.4. Modulul permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli. 20.5. Modulul permite/bloca accesul pentru înscriere și mlarea executabil. **21. Actualizare:** 21.1. Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare). **22. Scanarea vulnerabilităților infrastructurii:** 22.1. Soluția asigură scanarea vulnerabilitaților infrastructurii (echipamente din rețea, aplicațiilor web, etc) cu posibilitatea de a fi accesată dintr-o singură interfață. 22.2. Solutia este capabilă să identifice atat amenințările interne cât și externe și să raporteze riscurile, să ofere o vizibilitate a vulnerabilităților într-un mod centralizat pentru toate tipurile de dispozitive conectate în rețea și care pot	

					comunica, de exemplu: stații de lucru, servere, servere virtuale, site-uri, switch-uri, routere, aplicațiilor web, etc; 22.3. Solutia oferă posibilitatea de a identifica toate echipamentele conectate la rețea, la fel va fi posibil de a verifica tipul de echipament, după caz: sistemul de operare instalat, IP-ul și MAC adresa, cărui domeniu aparține, vulnerabilitățile depistate, software-ul instalat pe echipament, spațiul disponibil, tipul procesorului, tipul Bios-ului. 22.4. Soluția permite planificarea activităților după data/ora/an și de rulat scanarea vulnerabilităților pentru fiecare echipament în parte. 22.5. Soluția pune la dispozitie un instrument care poate fi instalat pe o mașină virtuală sau pe un calculator în rețeaua pe care se dorește o scanare al vulnerabilităților sau pentru colectarea datelor echipamentelor aflate în rețea. 22.6. Soluția permite adăugarea unui grup de scanare in care se va indica minim: Numele grupului si persoana responsabilă, descrierea succintă a grupului. 22.7. Posibilitatea de scanare prin alegerea unui șablon prestabilit care va propune scanarea sistemului după modelele: 22.7.1. Badlock detection; 22.7.2. Bash Shellshock detection; 22.7.3. GHOST detection; 22.7.4. Hearbeast detection; 22.7.5. PCI scan; 22.7.6. Scan full TCP/UDP port range; 22.7.7. Scan top- 100 ports; 22.7.8. Scan top-1000 ports; 22.7.9. SSL/TLS maturity scanning: 22.8. Modul de scanare sa poată fi setat după: ora, repetiiri zilnice, săptiimanale. lunare, trimestriale. etc. 22.9. Soluția poate fi administrată printr-o singură consolă, fără ca să necesite careva echipamente hardware (servere de management) sau careva software speciale. 22.10. Soluția propusă poate genera un raport pe segmente din rețea pe care se doreste, cu posibilitatea selectării vulnerabilitaților care vor fi afișate în raport, sortate după severitatea lor. 22.11. Soluția propusa pune la dispozitie posibilitatea de a asigna remedierea unei vulnerabilități către un user / administrator creat în platforma de administrare.	

"RTS ONE" S.R.L.
https://rts.md
(+373) 22 101 777
office@rts.one
str. Mitropolit G. Bănulescu-Bodoni 59/B, of. 815

					22.12. Consola de administrare suportă urmatoarele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome. 22.13. Soluția poate afișa toată informatia referitor la licența instalată și va jurnaliza evenimentele și modificările aplicate de către user-ul care are accesul la portal. 22.14. În consola de administrare se regăsește accesul la manuale, ghiduri de instalare, ghidul de utilizare, etc, informații referitor la schimbările și actualizările soluției, portal pentru suport cu posibilitatea de a solicita ajutor de la producator. 22.15. Solutia oferă scanări nelimitate pe parcursul perioadei de licență. **CERINTE FAȚĂ DE SERVICIILE DE IMPLEMENTARE și CONFIGURARE** **23. Caracteristici generale:** 23.1. În calitate de ofertant selectat vom livra si instala licențele pentru soluția ofertată. 23.2. În calitate de ofertant selectat vom efectua pregătirea mediului de instalare pentru soluția propusă, după care va asigura implementarea initială a solutiei aplicative in mediul de productie și mediul de testare. 23.3. În calitate de ofertant selectat vom efectua configurarea inițială a soluției, atât pentru mediul de producție, cât și mediul de testare. Prin configurare initială se întelege setarea tuturor parametrilor aplicabili in corespundere cu cerintele (clientului), inclusiv configurarea și instalarea solutiei ofertate, setarea politicilor și testarea înainte de a fi pusa în producție. 23.4. În baza rezultatelor de la etapa de design, în calitate de ofertant vom implementa toate configurările / customizările agreate și darea în exploatare a soluției. 23.5. În calitate de ofertant selectat vom efectua instalarea solutiei ofertate în intreaga intrastructură a Comisiei Nationale a Pietei Financiare, inclusiv la toți utilizatorii finali (instalarea se va considera încheiată în momentul cand toti utilizatorii vor avea instalat agentul și calculatorul va primi cel puțin o actualizare a bazelor și a agentului). 23.6. La sfarsitul etapei, în calitate de ofertant vom efectua o demonstrație a soluției ți a modulelor care au fost acoperite, fapt care va servi drept unul din criteriile de acceptanță ale etapei de implementare. 23.7. După acceptanță finală a soluției, va fi activată în mod automat opțiunea de garanție post- implementare și suport. Perioada de garantie post-implementare si suport va fi de 1 an calendaristic de la data activării acestui opțiuni.	

					23.8. Serviciile de garanție post-implementare și suport se referă la serviciile oferite de către Ofertantul selectat aditional la serviciile de mentenanță și suport a licențelor, oferite direct de către producătorul licențelor. 23.9. Serviciile de garanție post-implementare și suport, vor include următoarele componente: 23.9.1. Gestionarea serviciului de actualizare a serverelor la ultimele actualizări oferite de produciitor; 23.9.2. Gestionarea incidentelor de securitate apârute pe perioada suportului activ; 23.9.3. Solicitâri lor de schimbare a politicilor de securitate; 23.9.4. Solicitari de analiza si corectie a politicilor de securitate in cadrul companiei implementate. **24. Cerintele față de serviciile de instruire** 24.1. În cadrul proiectului, în calitate de ofertant vom organiza sesiuni de instruire și transfer de cunostinte pentru grupurile tintă in vederea formării setului de cunostinte necesar pentru a permite echipei instruite să preia mentinerea si configurarea ulterioară a soluției, în conformitate cu necesitățile utilizatorilor. 24.2. Instruirea se va organiza pentru diferite grupuri tintă la sediul Cumpărătorului. 24.3. Administrator - 3 persoane. 24.4. În acest sens, în calitate de ofertant vom prezenta ca parte a ofertei, un plan de instruire, în care se va indica ce tipuri de instruiri va efectua Ofertantul, pentru ce categorie de utilizatori, precum și cuprinsul/agenda acestor instruiri. 24.5. În afara instruirilor ce tin de utilizarea soluției, în calitate de ofertant vom efectueze și sesiuni de instruire pentru echipa de mentenanță din partea Cumpărătorului, in scopul asigurării unui nivel adecvat de cunostinte și competențe, pentru a putea utiliza eficient instrumentele de configurare si dezvoltare disponibile in cadrul solutiei. 24.6. În cadrul serviciilor de implementare, pentru a asigura transferul necesar de cunostinte către echipa Cumpărătorului, în calitate de ofertant va fi de acord ca cel putin o persoană sa asiste la lucrările de parametrizare / configurare, stabilite de comun acord de către Părti. 24.7. În calitate de ofertant selectat la etapa de încheiere a contractului, va trebui sa elaboreze si sa convină cu Cumpărătorul următoarele elemente ale componentei de instruire: 24.7.1. Strategia Ofertantului cu privire la instruire și programul de formare;	

"RTS ONE" S.R.L.
https://rts.md
(+373) 22 101 777
office@rts.one
str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

					24.7.2. Structura si componenta pachetului de cursuri pentru formare si a manualelor de studiu pentru fiecare categorie de utilizator; 24.7.3. Metodologia st procedurile de evaluare si control a1 eficientei si suficientei sesiunilor de instruire. 24.8. În cadrul sesiunilor de instruire, în calitate de ofertant va pune la dispoziția Cumpărătorului întreg setul de documentatie al solutiei care sa cuprindă cel putin urmñtoarele componente: 24.8.1. Ghidurile administratorilor; 24.8.2. Ghidurile de instalare și configurare; 24.8.3. Fisierele surse pentru toate configurările si customizările realizate pe parcursul proiectului. **25. Licențe:** 25.1. - 110 endpoints (fizice st virtualizate), 12 luni subscripție; 25.2. - 40 servers (fizice si virtualizate). 12 luni subscripție; 25.3. - 40 IP (interne, externe, web), 12 luni subscripție. **26. Cerinte minime de calificare a ofertantilor:** 26.1. Producătorul trebuie sa ofere suport tehnic 24/7, inclusiv in limba română prin e-mail sau telefon; 26.2. Suport tehnic local 24/7 în limba română din partea partenerului local; 26.3. Autorizarea de la Producător a partenerului vis-a-vis de dreptul de vânzare si de a oferi suport tehnic produselor ofertate pe teritoriul R.Moldova; 26.4. Prezentarea documentelor confirmative a minim 2 specialisti certificati pe solutia propusă.	
TOTAL						

Semnat:

Digitally signed by Celonenco Vitalie
Date: 2022.08.24 11:28:41 EEST
Reason: MoldSign Signature
Location: Moldova

Numele, Prenumele: **CELONENCO Vitalie**

În calitate de: **Administrator**

Ofertantul: **„RTS ONE" S.R.L.**

Adresa: **mun.Chișinău, str.Mitropolit Gavriil Bănulescu-Bodoni, 59/B, of.815**