Nr. IF2026-002283 / 13.05.2026

APROBAT
DIRECTOR EXECUTIV
Nițescu Carmina

Simu Ionut-Serban
Digitally signed by Simu Ionut-Serban
Date: 2026.05.13 15:48:05 +03'00'

CAIET DE SARCINI

1. OBIECTUL CONTRACTULUI

Autoritatea contractantă doreşte să achiziţioneze o prelungire la licenţe informatice deţinute de instituţie pentru care se solicită prelungirea valabilităţii:

LOT	DENUMIRE	DATA EXPIRARE	CPV	SERIE	CANTITATE
Lot I	Prelungire licenta Next Generation Firewall 36 luni	31.08.2026	48219000-6	12001004813	1
Lot II	Prelungire licenta DUO Essentials(130 de utilizatori) - 3 ani	29.06.2026	48700000-5	-	130
Lot III	Prelungire licenta soft de inventariere(1 an)	01.07.2026	48781000-6	WSWLGJKK QUZ1UNU	1
Lot IV	Prelungire licenta antivirus 130(endpont-uri) - Endpoint EDR - 1 an	24.07.2026	48760000-3	-	130
Lot V	Prelungire Licenta Windows Server Standard License+Software Assurance 3 ani, OLP Licenta- 3 ani	31.08.2026	48620000-0	V3972997	24
Lot VI	Prelungire licenta soft acces de la distanta(Any Desk) - 24 luni	04.06.2026	48514000-4	-	1

2. SPECIFICAŢII TEHNICE

LOT I - Prelungire licența Next Generation Firewall 36 luni – 1 buc

Cantitate: 1 (pentru echipamentul PA-820)
Perioada: 36 luni, începand cu 01.09.2026
Funcționalități licențiate:

- Servicii de suport software oferit de producător prin update-uri și upgrade-uri automate ale sistemului de operare PAN-OS;
- Servicii de suport hardware pentru defecțiuni cu înlocuire în regim Next Business Day, susținut de producătorul echipamentului;
- Funcționalitate software de tip “Threat Prevention” pentru protejarea traficului de internet împotriva aplicațiilor de tip malware, ;
- Funcționalitate software de tip URL Filtering, pentru blocarea accesului la site-uri cu reputație malițioasa sau a acelora cu conținut nepotrivit.

Autoritatea contractantă dorește reînnoirea licenței de pe echipamentul **Palo Alto 820** aflat în infrastructura proprie. În situația în care producătorul Palo Alto Networks a redenumit, restructurat

sau înlocuit această licență cu un produs/pachet successor ori echivalent funcțional (inclusiv, dar fără a se limita la, integrarea funcționalităților în cadrul unui alt tier de licențiere, a unui pachet de tip *Advanced Threat Prevention, Advanced WildFire* sau orice altă denumire comercială adoptată ulterior de producător), ofertantul va furniza licența curentă oferită de Palo Alto Networks care asigură cel puțin același nivel de protecție și funcționalități ca licența **Threat Prevention** activă la momentul inițierii procedurii de achiziție. Licența ofertată trebuie să fie compatibilă cu echipamentele/platforma existentă în infrastructura achizitorului și să asigure continuitatea protecției fără întreruperi, indiferent de denumirea comercială sub care este comercializată de producător la data livrării.

LOT II - Prelungire licenta DUO Essentials(130 de utilizatori) – 3 ani

a) Prezentare Generală a Licenței actuale - Cisco DUO MFA

Soluția Cisco DUO MFA oferă o soluție robustă de autentificare multifactor (MFA) menită să asigure o securitate sporită a accesului la aplicații, în special pentru utilizatorii care se conectează de la distanță. Aplicația este proiectată pentru a facilita autentificarea dual, asigurând verificarea identității printr-un al doilea factor de securitate, astfel încât accesul la resursele instituției să fie permis doar după confirmarea identității utilizatorului printr-un dispozitiv terț.

Aplicatia este deja implementata pentru accesul de tip VPN Dial-In, integrarea este făcută cu Active Directory-ul local iar terminalele sunt înrolate.

b) Funcționalități și caracteristici tehnice specifice

- **Metode de Autentificare:**
  - **Client Multifactor de tip Push:** Permite autentificarea rapidă prin notificări push trimise către aplicația Duo Mobile pe platformele Android și iOS.
  - **Metode Alternative:** Suport pentru autentificare prin SMS, apel telefonic (callback), precum și generarea de coduri de securitate prin rotație de tip one-time-password (OTP).
  - **Flux Simplificat de Autentificare:** Asigură o experiență fluidă pentru utilizatori, minimizând întreruperile și facilitând adoptarea rapidă.
- **Integrare și Compatibilitate:**
  - **Protocoale și Sisteme de Identitate:** Integrare ușoară cu Microsoft Active Directory, printr-un portal de auto-enrolare, și suport pentru protocoale standard (LDAP, SAML, OIDC), facilitând astfel conectivitatea la diverse aplicații.
  - **Mecanism SSO (Single Sign-On):** Permite accesul centralizat la aplicații, eliminând necesitatea autentificărilor multiple și îmbunătățind experiența utilizatorilor.

c) Cerințe tehnice și de integrare în mediul remote al autorității contractante

- **Compatibilitate cu metodele de acces existente:**
  Soluția trebuie să fie compatibilă cu:
  - Acces VPN de tip Dial-In, utilizând gateway-ul PaloAlto Networks PA820 și clientul de conectare GlobalProtect;
  - Acces VPN de tip Dial-In tradițional;
  - Acces de tip Remote Desktop, destinat administrării platformei de servere.
- **Integrare nativă:**
  - Aplicația DUO MFA trebuie să integreze nativ cele trei categorii de acces menționate, asigurându-se că fiecare tip de conexiune beneficiază de protecția multifactor și de aplicarea politicilor de securitate.
- **Politici de securitate și management:**
  - Implementarea unor politici de securitate diferențiate, aplicate în funcție de grupuri și aplicații, cu posibilitatea de configurare ușoară prin intermediul consolei de administrare.

- Administratorii IT vor putea gestiona înscrierea și modificarea utilizatorilor prin actualizarea unui Security Group din cadrul Active Directory, noii membri fiind automat solicitați pentru configurarea celui de-al doilea factor de autentificare.

- **Implementare și integrare în infrastructura existentă:**
  - Furnizorul va instala și configura/prelungi aplicația pe o platformă virtuală de tip VMware disponibilă în cadrul autorității contractante;
  - Configurarea integrărilor se va face cu echipamentul Firewall și cu serviciul Microsoft RDP, pentru a solicita autentificare multifactor unui număr prestabilit de utilizatori (130 utilizatori, incluzând administratori de sistem, operatori de servicii și utilizatori remote);
- **Managementul dispozitivelor:**
  - Înrolarea și managementul dispozitivelor trebuie să fie simple și eficiente, astfel încât departamentul IT al autorității să poată administra rapid și intuitiv configurațiile, fără a necesita intervenții complexe.

d) Aspecte de Licențiere și Suport

- **Modelul de licențiere:**
  - Licența Cisco DUO MFA este oferită ca și pachet/serviciu de tip subscripție, tarifată, și este scalabilă pentru a acoperi necesarul de 130 de utilizatori;
  - Termenul de abonament pentru care este dorit serviciul - 36 luni, incluzând suportul și update-urile software aferente.
- **Suport și subscripție software:**
  - Oferta include suport tehnic și actualizări continue ale aplicației, asigurând astfel menținerea nivelului optim de securitate și performanță a soluției implementate.

Prezenta achiziție nu implică vendor lock sau exclusivitate tehnologică. În cazul în care alte soluții de la producători diferiți (cu denumiri trademark proprii) oferă aceleași funcționalități și îndeplinesc cerințele tehnice specificate de Autoritatea contractantă, aceștia pot propune propria licență și soluție de autentificare dual㠠. Orice ofertă alternativă trebuie să asigure respectarea tuturor cerințelor tehnice impuse, să furnizeze serviciile necesare și să acopere costurile asociate cu schimbarea soluției utilizate (fără aplicarea unui down-time al rețelei) în infrastructura actuală, garantând astfel o tranziție fără impact asupra securității și funcționalității sistemului existent.

Serviciile necesare trebuie sa includa (dar fara a se limita la):

- Integrarea terminalului de VPN PaloAlto Networks PA820 in soluția de autentificare;
- Inrolarea tuturor terminalelor utilizatorilor (suport pentru înrolarea de la distanta);
- Integrare cu Active Directory și politicile de acces aplicabile;

LOT III – Prelungire licență Soft de inventariere (1 an)

Softul de inventarierea aflat în exploatarea autorității contractante este la momentul actual – Lansweeper.

Soluția de prelungire/noua licență ofertată trebuie să fie în conformitate cu specificațiile tehnice detaliate mai jos, acoperind o gamă largă de funcționalități esențiale pentru descoperirea, gestionarea și monitorizarea echipamentelor și sistemelor din rețea. De la descoperirea automată și management-ul echipamentelor prin SNMP și până la integrarea cu Active Directory și alte mecanisme alternative de gestionare a sistemelor, fiecare cerință este formulată în vederea asigurării unei soluții robuste și scalabile.

În cazul în care soluția ofertată este alta decât Lansweeper, oferta trebuie să cuprindă serviciile de implementare necesare pentru punerea în funcțiune a soluției, precum instalarea locală, integrarea în infrastructura existentă și validarea rezultatelor inițiale împreună cu echipa Autorității Contractante. Prin intermediul acestor cerințe tehnice și a serviciilor asociate, se urmărește garantarea implementării eficiente și a utilizării optime a soluției în cadrul instituției.

Caracteristici tehnice:

- **Descoperire automată și management al echipamentelor**: Soluția oferită trebuie să permită identificarea automată și management-ul echipamentelor și sistemelor din rețea, folosind protocolul SNMP, fără a necesita furnizarea credențialelor de acces;
- **Descoperire pasivă și activă**: Soluția trebuie să ofere atât descoperire pasivă, bazată pe broadcast-urile emise de echipamentele care se conectează la rețea, cât și descoperire activă prin scanarea segmentelor de rețea specificate, fără a necesita furnizarea de credențiale. Nu este necesară instalarea de programe suplimentare pe echipamentele și sistemele din rețea pentru implementarea soluției – cu excepția situației în care echipamentele gestionate nu sunt prezente în rețeaua locală, sunt deconectate sau sunt protejate de un firewall strict configurat, când se poate instala un agent;
- **Utilizare a informațiilor de tip "switchport"**: Soluția trebuie să poată identifica echipamentele folosind informații de tip "switchport" și să genereze topologii de conectare evidențiind portul fizic și switch-ul asociat acestuia;
- **Detectare automată a echipamentelor conectate la switch-uri**: Trebuie să permită detectarea tuturor echipamentelor conectate în porturile unui switch și să listeze automat adresele MAC, IP și numele host-urilor acestora;
- **Colectare de date detaliată**: Soluția trebuie să permită colectarea de date detaliate legate de echipamentele și sistemele din rețea, inclusiv specificații hardware, software instalat, detalii despre utilizatori etc;
- **Inventariere completă**: Trebuie să fie capabilă să ofere un inventar detaliat al tuturor componentelor hardware, software și utilizatorilor din organizație, inclusiv informații despre producător, model și sistem de operare;
- **Capacitatea de gestionare a unui număr mare de echipamente**: Soluția trebuie să permită inventarierea a până la 500 de asset-uri și sisteme, inclusiv stații de lucru, servere fizice sau virtuale, echipamente de stocare, imprimante etc;
- **Integrare cu Active Directory și alte mecanisme alternative**: Soluția trebuie să permită inventarierea și scanarea calculatoarelor și utilizatorilor înrolați în Active Directory, precum și integrarea cu alte mecanisme alternative de gestionare a sistemelor, cum ar fi Microsoft Intune, SCCM, Airwatch etc;
- **Colectare automată a informațiilor despre garanția hardware**: Prin interogarea automată a portalurilor cu date specifice, soluția trebuie să fie capabilă să colecteze informații despre garanția hardware a sistemelor de la producătorii majori (HP, Dell, Lenovo, Fujitsu).
- **Management complet al imprimantelor**: Soluția trebuie să permită detectarea nivelului de încărcare al cartușelor, informații despre producător, model, interfețe de rețea etc.
- **Administrare și actualizare software**: Trebuie să permită instalarea, dezinstalarea și actualizarea programelor software, precum și modificarea liniilor de comandă, închiderea proceselor și rularea de scripturi;
- **Scanări programate și actualizări periodice**: Soluția trebuie să permită scanări programate în rețea și actualizarea bazei de date cu atributele echipamentelor, evidențiind dispozitivele noi sau neautorizate;
- **Normalizare și prezentare a rapoartelor**: Trebuie să ofere normalizarea informațiilor și prezentarea rapoartelor semnificative pentru diferitele tipuri de sisteme de operare, versiuni de aplicații, firmware, configurații hardware etc;
- **Detectare a vulnerabilităților**: Trebuie să ofere informații referitoare la vulnerabilitățile descoperite în versiunile software instalate, folosind catalogul NIST;
- **Raport de uptime și monitorizare grafică**: Trebuie să ofere un raport de uptime privind utilizarea activă a echipamentelor, cu posibilitatea de a monitoriza grafic timpul de utilizare al fiecărui echipament;
- **Management remote/de la distanță**: Trebuie să permită rularea unor acțiuni pe echipamentele gestionate, cum ar fi restartul, shutdown-ul, consultarea Event Viewer-ului, ping, traceroute etc;
- **Instalare automată de software-uri**: Soluția propusă trebuie să permită instalarea automată a unor software-uri (aplicații noi, patch-uri) din consola de gestionare pentru sistemele

detectate (ce sunt compatibile cu astfel de tehnologii), precum și posibilitatea de a implementa agenți de la alte soluții software (de ex. agenți pentru data aquisition în cazul unei soluții de tip SIEM);

Prezenta achiziție nu implică vendor lock sau exclusivitate tehnologică. În cazul în care alte soluții de la producători diferiți (cu denumiri trademark proprii) oferă aceleași funcționalități și îndeplinesc cerințele tehnice specificate de Autoritatea contractantă, aceștia pot propune propria licență și soluție de inventariere. Orice ofertă alternativă trebuie să asigure respectarea tuturor cerințelor tehnice impuse, să furnizeze serviciile necesare și să acopere costurile asociate cu schimbarea soluției utilizate (fără aplicarea unui down-time al rețelei) în infrastructura actuală, garantând astfel o tranziție fără impact asupra securității și funcționalității sistemului existent.

Licențierea: licenta perpetua sau pe baza de subscriptie software valabil cel putin 12 luni, care sa acopere intreaga platforma a autoritatii contractante:

- 140 utilizatori interni, 20 utilizatori externi
- Pana la 500 assset-uri (calculatoare, imprimante, AP-uri, switch-uri, rutere, alte echipamente conectate la retea)

LOT IV - Prelungire licenta antivirus 130(endpont-uri) - Endpoint EDR - 1 an

Autoritatea contractantă dorește prelungirea prin adaugarea de facilitati sau achiziția unei platforme de protecție pentru terminalele/stațiile (end point) angajaților ce combină măsuri de prevenție și detecție – printr-o abordarea dual de tip Platformă centrală de protecție (Endpoint Protection Platform) + tehnologie de tip EDR (Endpoint Detection and Response) – pentru a asigura un nivel ridicat de securitate într-un mediu IT modern.

Soluția trebuie să utilizeze un antivirus de ultimă generație, alimentat de algoritmi de inteligență artificială, ce permite identificarea și blocarea rapidă a amenințărilor cunoscute și necunoscute(NGAV). În plus, aceasta trebuie să includă funcționalități esențiale precum monitorizarea și gestionarea dispozitivelor IoT neautorizate, controlul traficului prin firewall, restricții și gestionare a accesului la periferice și porturi (Device Control) și posibilități de acces la nivel de Remote Shell pentru intervenții de urgență. Mai mult, soluția dispune de capabilități avansate de "threat hunting" și investigație, oferind instrumente analitice ce permit identificarea proactivă a comportamentelor anormale și neutralizarea rapidă a incidentelor de securitate. Acest ansamblu tehnologic asigură o protecție completă și adaptată la dinamica amenințărilor cibernetice actuale, contribuind la menținerea integrității și disponibilității infrastructurii IT.

Oferta trebuie să cuprindă serviciile de implementare necesare pentru punerea în funcțiune a noi solutii, sau a extinderii functionalităților soluției existente, precum instalarea locală, integrarea în infrastructura existentă și validarea rezultatelor inițiale împreună cu echipa Autorității Contractante. Prin intermediul acestor cerințe tehnice și a serviciilor asociate, se urmărește garantarea implementării eficiente și a utilizării optime a soluției în cadrul instituției.

Din perspectiva cerințelor tehnice, aceasta ar trebuie să îndeplinească minim următoarele:

	Componenta de protectie a statiilor
1.1.	Componenta de administrare trebuie sa fie livrata sub forma de serviciu in cloud.
1.2.	Solutia trebuie sa fie dimensionata pentru protectia a cel putin 130 sisteme, pe o perioada de 12 luni
1.3.	Intreaga functionalitate a solutiei trebuie sa fie administrata cu ajutorul componentei de management în cloud, configurarea fiind realizata cu ajutorul unui browser web, fara a avea nevoie de aplicații suplimentare;
1.4.	Solutia trebuie să ofere API-uri pentru integrarea bidirectionala cu soluții de securitate terte
1.5.	Solutia trebuie să includă mecanisme de autentificare prin cel putin 2 metode;
1.6.	Agentul trebuie să protejeze cel puțin următoarele tipuri de sisteme de operare : Windows (inclusiv Win 7 SP1, Windows Storage Server) , macOS, Linux

1.7.	Agentul trebuie sa fie capabil să protejeze cel puțin următoarele platforme de administrare a containerelor : Kubernetes, OpenShift
1.8.	Platforma trebuie să asigure o conexiune de tip remote shell pentru investigarea de la distanta a stațiilor, protejată cu o parola dedicata sesiunii respective și care să includă istoricul comenzilor executate;
1.9.	Agentul trebuie să includă funcționalități de tip EPP (endpoint protection) și EDR (endpoint detection and response) integrate în cadrul unui singur pachet software;
1.10.	Platforma trebuie să asigure un control granular al dispozitivelor externe de tip USB și Bluetooth folosind următoarele restrictii: - USB : read + write, read only sau block. - Bluetooth: allow sau block , inclusiv în funcție de versiunea protocolului folosit (ex. de la 2.1 pana la 5.1)
1.11.	Agentul instalat trebuie să protejeze sistemul în cazul în care acesta nu este conectat la internet
1.12.	Soluția trebuie să ofere următoarele acțiuni de remediere, care pot fi executate manual sau automat în cadrul politicilor: - Oprirea proceselor; - Carantinarea amenințărilor; - Ștergerea fișierelor și a modificărilor sistemului cauzate de atac; - Pentru sistemele de operare Microsoft Windows, există opțiunea de a restaura sistemul la o stare anterioară infectării cu malware;
1.13.	Solutia trebuie să detecteze atacuri care rulează în memoria sistemului;
1.14.	Solutia trebuie să includă un mecanism de detecție dinamică a atacurilor, fără a fi necesara utilizarea unei solutii de tip sandbox;
1.15.	Soluția trebuie să includă un modul care colecteaza, stocheaza și analizează date provenite de la agenții instalați sau de la solutii externe (cel putin 10 GB/zi de date inclusi). Perioada de stocare a datelor trebuie sa fie de minim 14 zile, extensibila pana la cel putin 12 luni.
1.16.	Soluția trebuie să ofere un modul care utilizează tehnici de inducere în eroare a atacatorilor, precum honeypots (capcane digitale) sau alte sisteme de diversiune, cu posibilitatea de carantinarea automata a atacului ;

Prezenta achiziție nu implică vendor lock sau exclusivitate tehnologică. În cazul în care alte soluții de la producători diferiți (cu denumiri trademark proprii) oferă aceleași funcționalități și îndeplinesc cerințele tehnice specificate de Autoritatea contractantă, aceștia pot propune propria licență și soluție de antivirus. Orice ofertă alternativă trebuie să asigure respectarea tuturor cerințelor tehnice impuse, să furnizeze serviciile necesare și să acopere costurile asociate cu schimbarea soluției utilizate (fără aplicarea unui down-time al rețelei) în infrastructura actuală, garantând astfel o tranziție fără impact asupra securității și funcționalității sistemului existent.

LOT V - Prelungire Software Assurance pentru Microsoft Windows Server Standard Core, 2 Core License

Continuarea valabilității Licențelor Windows Software Assurance (SA) aduc o serie de beneficii și avantaje, inclusiv acces la upgrade-uri și actualizări ale sistemului de operare Windows, suport tehnic, flexibilitate în licențiere, servicii de planificare și implementare reprezentând o cale de optimizare a costurilor pe termen lung. Acest tip de licențe permite organizațiilor să mențină infrastructura IT actualizată, să beneficieze de flexibilitate în utilizarea dispozitivelor și să primească suport în implementarea și gestionarea upgrade-urilor, aspecte esențiale în funcționarea serviciilor Autorității contractante.

Prin prezenta se cere achiziția unei prelungiri a serviciului Microsoft de Software Assurance pentru 3 ani incepand cu 01.09.2026 pentru licentele Microsoft Windows Server Standard Core detinute. Directia Fiscala a Municipiului Timisoara detine 24 pachete a cate 2 licente / nucleu.

- **Cantitate**: 24 pachete a cate 2 licente / nucleu (1 licentă la 2 nuclee)
- **Perioada**: 3 ani, începând cu 01.09.2026

LOT VI – Prelungire licenta Soft acces de la distanță(Any Desk)

Caracteristicile tehnice au rolul de a stabili standardele și specificațiile necesare pentru a asigura funcționarea corespunzătoare a soluției, precum și pentru a îndeplini cerințele operaționale și de securitate ale organizației.

Caracteristici tehnice:

- **Partajare ecranului, versiuni și securitatea aferentă:**
  - Utilizatorul trebuie să poată partaja ecranul echipamentului în mod interactiv cu un agent de helpdesk;
  - Canalul de comunicare a datelor trebuie să fie securizat, fără a necesita modificări în regulile de firewall sau politicile de domeniu;
  - Soluția trebuie să fie compatibilă cu toate versiunile de Windows (8, 10, 11);
  - Solutia trebuie sa fie compatibila cu versiunile actuale de Android si iOS pentru telefoane mobile;
  - Stabilirea conexiunii rapide prin introducerea unui cod unic sau a unui alias predefinit, chiar și în cazul utilizatorilor cu privilegii restrânse (non-administratori locali);
- **Codec-uri eficiente pentru transmisie.** Soluția trebuie să asigure utilizarea de codec-uri eficiente pentru comprimarea imaginilor afișate, permițând funcționarea optimă în medii cu conexiuni la internet reduse, astfel încât partajarea ecranului să poată fi făcută și din locații cu o infrastructură de internet deficitară;
- **Interacțiune interactivă.** Soluția trebuie să vină cu opțiunea de schimb de mesaje în timp real între agent și utilizator pentru interacțiunea eficientă și constată pe toată perioada sesiunii de partajare a ecranului;
- **Transfer de fișiere și clipboard integrat.** Software-ul propus trebuie să aibă posibilitatea de transfer de fișiere între cele două sisteme de operare conectate (agentul ce acordă helpdesk-ul și utilizatorul neavizat), inclusiv un clipboard transferabil;
- **Înregistrare a sesiunii de suport.** Soluția trebuie să vină cu capacitatea de a înregistra sesiunea de suport stabilită pentru scopuri de audit și urmărire a activității de către Autoritatea Contractantă;
- **Conectare neasistată.** Instalarea prealabilă a unui agent software pe stațiile de lucru, permițând conectarea automată prin simpla selectare a destinației și introducerea unei parole de acces predefinite;
- **Integrare cu Autentificare Dual-Factor.** Posibilitatea de integrare cu mecanisme de autentificare dual-factor pentru accesul la sisteme sensibile;
- **Funcționare ca Serviciu Windows.** Agentul trebuie să poată rula sub forma de „service", asigurând accesibilitatea automată chiar și după repornirea sistemului;
- **Conectare Externă.** Conectarea trebuie să fie posibilă chiar și când utilizatorul nu se află în rețeaua internă a organizației, fără o conexiune VPN stabilă, dar cu acces la internet;
- **Tehnologie de tip Wake-On-LAN integrată.** Soluția trebuie să vină cu posibilitatea de a porni sistemele folosind funcția Wake-On-LAN, integrată în consola soluției de administrare pentru gestionarea eficientă a echipamentelor;

Licențierea:

Solutia trebuie să fie licențiată fie în model perpetuu, fie în model bazat pe subscripție software pentru o perioada de cel putin 24 luni.

Licența trebuie să fie valabila pentru un număr de cel puțin 130 echipamente administrate.

Aplicația nu trebuie să aibă limitări la durata unei sesiuni de suport, sau la numarul de sesiuni înregistrate către același echipament.

Fiecare ofertant trebuie să nominalizeze soluția software propusă, să prezinte datasheet-uri de pe site-ul producătorului care să dovedească respectarea cerințelor.

Furnizorul va instala modulele aplicației în rețeaua Autorității Contractante și va demonstra capabilitățile soluției făcând sesiuni de suport atât cu sisteme de operare de tip Windows cat și către telefoane mobile.

3. TERMENE ŞI CONDIŢII DE LIVRARE

Operatorii economici desemnaţi căştigători vor livra softurile și licenţele în termen de cel mult 10 zile(calendaristice) de la semnarea contractului.

La livrare, produsele vor fi însoţite de următoarele documente:

a) factură în original;
b) declaraţie de conformitate în original;

4. RECEPŢIE

Recepţia va fi efectuată la sediul Achizitorului, după livrare, în termen de maxim 5 zile lucrătoare.

Dacă, în urma inspecţiilor şi testelor, produsele corespund specificaţiilor din ofertă, se va încheia procesul-verbal de recepţie.

Dacă produsele nu corespund specificaţiilor din ofertă, pe baza procesului-verbal de reclamaţie, achizitorul are dreptul să îl respingă, iar furnizorul are obligaţia ca în termenul de livrare şi fără a modifica preţul:

a) de a înlocui produsul refuzat; sau
b) de a face toate modificările necesare pentru ca produsul să corespundă specificaţiilor tehnice.

5. MODLITĂŢI DE PLATĂ

Plata se va efectua de către Achizitor, în lei, prin ordin de plată, pe baza următoarelor documente:

a) factură în original;
b) document de recepţie;
c) declaraţie de conformitate în original.

Plata facturii se va efectua în maxim 30 de zile calendaristice de la recepţie *conform prevederilor Legii nr. 72/2013,* în contul de Trezorerie al furnizorului.

Compartiment Achiziții Publice
Bunea Gheorghe

Bunea Gheorghe
Digitally signed by Bunea Gheorghe
Date: 2026.05.13 15:31:54 +03'00'