Nr. 5662 din 27.06.2026

ANUNŢ

Institutul Inimii de Urgență pentru Boli Cardiovasculare „Niculae Stăncioiu" este interesat să achiziționeze "Furnizare, instalare și punere în funcțiune sistem integrat de securitate pentru Lab. Angiografie, Compartiment Electrofiziologie și Ambulator, bazat pe platformă software unificată scalabilă și infrastructură server în cadrul Institutului"

Cod CPV: 35125000-6 Sisteme de supraveghere

Tip contract: Contract de lucrări de instalații electrice

Valoare estimată: 32.300,00 lei

Modalitate de desfășurare: Conform art. 7 alin. (7) lit. a) din Legea 98/2016 care stabilește că :" În cazul achiziţiei directe, autoritatea contractantă:

a) are obligaţia de a utiliza catalogul electronic pus la dispoziţie de SEAP sau de a publica un **anunţ într-o secţiune dedicată a website-ului propriu** sau al SEAP, însoţit de descrierea produselor, serviciilor sau a lucrărilor care urmează a fi achiziţionate, pentru achiziţiile a căror valoare estimată este mai mare de 200.000 lei, fără TVA, pentru produse şi servicii, respectiv 560.000 lei, fără TVA, pentru lucrări", cu respectarea principiilor de transparență, eficiență, tratament egal și utilizare judicioasă a fondurilor publice.

Scopul achiziției:

Scopul achiziției îl reprezintă furnizarea, instalarea, configurarea, testarea și punerea în funcțiune a unui sistem integrat de securitate destinat Laboratorului de Angiografie, Compartimentului de Electrofiziologie și Ambulatoriului, în vederea asigurării protecției personalului, pacienților, echipamentelor medicale și infrastructurii aferente, precum și monitorizarea și controlul accesului în spațiile vizate.

Achiziția urmărește creșterea nivelului de securitate operațională, prevenirea accesului neautorizat, asigurarea trasabilității accesului și conformarea cu cerințele legale și standardele aplicabile unităților medicale.

Furnizarea și instalarea sistemelor de supraveghere video sunt necesare pentru a asigura siguranța pacienților, monitorizarea accesului pentru prevenirea incidentelor, protecția bunurilor și a personalului, precum și respectarea Legii nr. 159 din octombrie 2025, iar camerele video vor fi amplasate astfel încât să asigure monitorizarea continuă a activităților medicale medicale și ale pacienților, fără a compromite intimitatea acestora, cu respectarea legislației privind protecția datelor cu caracter personal și drepturile pacienților.

Condiții de recepție:

Recepția se va efectua în două etape:

a) Recepția cantitativă și de punere în funcțiune (Etapa 1) – se efectuează la finalul Etapei 1 (max. 10 zile lucrătoare), pe baza:

- Verificării livrării tuturor echipamentelor și materialelor conform devizului confirmat de Serviciul Tehnic
- Facturii, declarației de conformitate, certificatelor de garanție
- Testării funcționale a tuturor camerelor, înregistrării, accesului centralizat, alarmelor și privacy mask-urilor
- Verificării integrării în rețeaua locală și în sistemul de supraveghere centralizat
- Bifării checklist-ului pentru regimul de sistem închis

b) Recepția finală (Etapa 2) – se efectuează după predarea integrală a documentației și a instruirii personalului (max. 5 zile lucrătoare suplimentare după recepția Etapei 1), și NUMAI dacă:

- Documentația tehnică completă a fost predată în 2 exemplare originale + format electronic, conform listei de la pct. 6
- Instruirea personalului a fost efectuată și consemnată în proces-verbal semnat de participanți
- Nu sunt identificate neconformități față de cerințele caietului de sarcini

Recepția finală se face doar dacă sistemele funcționează conform cerințelor și nu sunt identificate neconformități. În caz contrar, se acordă termen pentru remedieri, cu reluarea procesului de recepție.

Executantul va deține autorizație IGPR pentru instalare sisteme de securitate (Legea nr. 333/2003) – copie după licență se va anexa la ofertă

Operatorii care intervin pe partea de configurare rețea / IT vor avea minim certificare de bază pe echipamentele ofertate (atestat producător sau echivalent)

Pretul ofertei:

Ofertanții vor cuprinde în calculul prețurilor unitare toate cheltuielile necesare furnizării și punerii în funcțiune prevăzute (cheltuieli cu manipularea materialelor, cheltuieli de transport etc.)

Notă: departajarea se va face exclusiv în funcție de preț și nu prin cuantificarea altor elemente de natură tehnică sau alte avantaje care rezultă din modul de îndeplinire a contractului de către operatorii economici în vederea departajării ofertelor, autoritatea contractantă va solicita depunerea unor noi propuneri financiare îmbunatățite, iar operatorii economici vor transmite răspunsul lor, caz în care contractul va fi atribuit ofertantului care a prezentat prețul cel mai scăzut.

Plata se va face în termen de 60 de zile de la emiterea facturii, după semnarea procesului-verbal de recepție finală fără obiecțiuni. Plata va fi realizată după alocarea fondurilor necesare de către autoritatea contractantă și în conformitate cu procedurile contabile și legislative aplicabile.

Valabilitatea ofertei: minim 90 zile

Criterul de atribuire: ***Pretul cel mai scăzut*** în conformitate cu prevederile art.187, alin. (3), lit. d) din Legea nr. 98/2016, cu condiția respectării tuturor cerintelor caietului de sarcini. Alegerea acestui criteriu urmărește **asigurarea utilizării eficiente a fondurilor publice**, cu respectarea cerințelor tehnice și funcționale impuse de autoritatea contractantă, în condițiile unei oferte conforme din punct de vedere tehnic.

Contractantul va asigura: livrare, instalare, configurare, integrare, testare, punere în funcțiune și instruirea personalului desemnat de beneficiar, în termenul asumat prin ofertă.

La recepție, contractantul va preda în mod obligatoriu: documentația tehnică finală, schema de principiu / as-built, licențele, credențialele de administrare predate în regim controlat, procese-verbale de testare și punere în funcțiune.

Garanția minimă este cea prevăzută în caietul de sarcini, cu obligația asigurării remedierii defecțiunilor în perioada de garanție, conform termenelor asumate contractual.

Informații suplimentare: **Vizita obligatorie la fața locului:** ofertanții sunt **OBLIGAȚI** să efectueze o vizită la fața locului **ÎNAINTE** de depunerea ofertei, pentru evaluarea condițiilor concrete de instalare, a traseelor de cablu și a punctelor de conectare în rețea. Vizita se programează telefonic la Serviciul Administartiv al Institutului. Ofertele depuse fără efectuarea acestei vizite nu vor fi luate în considerare.

Ofertanții vor trimite oferta în **PLIC ÎNCHIS** până în data de **02.06.2026, ora 11:00.**

MANAGER,

Jr.Florin CRIȘAN

COMP.ACHIZITII PUBLICE,

Ec.Lucreția LOBODĂ

APROB
MANAGER
Jr. Florin CRIȘAN

CAIET DE SARCINI

1. Obiectul achiziției

Furnizare, instalare și punere în funcțiune sistem integrat de securitate pentru Lab. Angiografie, Compartiment Electrofiziologie și Ambulator, bazat pe platformă software unificată scalabilă și infrastructură server în cadrul Institutului.

2. Tabel centralizator

Nr. Crt.	Denumire	U.M	Cantitate	Preț unitar estimat lei fără TVA	Valoare estimată lei fără TVA
1	Furnizare, instalare și punere în funcțiune sistem integrat de securitate pentru Lab. Angiografie, Compartiment Electrofiziologie și Ambulator	buc	1	32.300,00	32.300,00
TOTAL FĂRĂ TVA					**32.300,00**
Elemente componente:					
1.1	Camere supraveghere video color IP 5MP	buc	10		
1.2	Server video	buc	1		
1.3	Platformă integrare software pentru camere video	buc	1		
1.4	Licențe interconectare camere video la platforma integrată	buc	10		

3. Specificații tehnice

Sistemul propus va include camere video IP cu analiză inteligentă și platformă software unificată pentru management video, monitorizare, arhivare și raportare.

Se furnizează și se instalează toate materialele, licențele, accesoriile, serviciile de configurare și punere în funcțiune. Camerele video se montează în 3 săli Lab. Angiografie, 2 camere în Compartiment Electrofiziologie și 5 camere în sala de așteptare Ambulator parter.

- *Cerințe minime platformă software – conform fișa tehnică 1*

Platforma software trebuie să pernită integrarea tuturor echipamentelor de securitate existente din cadrul institutului, acestea având producători diferiți pentru a gestiona sistemul unitar al echipamentelor de securitate.

Integrarea acestor sisteme pe platforma software trebuie să respecte :

- principiile Privacy by Design și Privacy by Default, conform art.25 GDPR,
- securitatea prelucrării datelor conform art.32 GDPR,
- drepturile persoanelor vizate, art. 15-22 GDPR

- *Cerințe minime camere video (interior) – conform fișa tehnică 2*
- *Cerințe minime server video – conform fișa tehnică 3*
- *Cerințe minime licență interconectare camere video în platformă – conform fișa tehnică*

4. Criteriu de atribuire și factori de evaluare

Criteriul de atribuire este prețul cel mai scăzut, care se va aplica pentru ofertele care îndeplinesc cerințele minime și obligatorii din prezentul caiet de sarcini.

5. Termen de garanție

Garanția echipamentelor este de minim 24 de luni de la recepția facturii. În această perioadă prestatorul asigură GRATUIT remedierea defecțiunilor și a pieselor de schimb.

- Timp maxim de răspuns la solicitare: 6 ore în zilele lucrătoare
- Timp maxim de remediere: 24 de ore de la sesizare; pentru defecțiuni complexe se poate prelungi cu acordul beneficiarului, cu asigurarea unui echipament de schimb în regim loaner

Remedierea echipamentelor defecte se va executa, de regulă, la fața locului, la sediul beneficiarului. În cazuri speciale de reparații complexe, acestea se pot executa la sediul prestatorului, cu transportul în sarcina prestatorului.

6. Termen de executare și alte mențiuni

Vizita obligatorie la fața locului: ofertanții sunt OBLIGAȚI să efectueze o vizită la fața locului ÎNAINTE de depunerea ofertei, pentru evaluarea condițiilor concrete de instalare, a traseelor de cablu și a punctelor de conectare în rețea. Vizita se programează telefonic la Serviciul Administartiv al Institutului. Ofertele depuse fără efectuarea acestei vizite nu vor fi luate în considerare.

Termen de execuție: termenul se structurează pe două etape distincte:

- Etapa 1 – Instalare și punere în funcțiune: maximum 10 zile lucrătoare de la semnarea contractului. Include livrarea echipamentelor, montarea, cablarea, configurarea, integrarea în rețea și în sistemul de supraveghere centralizat, configurarea regimului de

sistem închis (GDPR) și testarea funcțională în prezența beneficiarului. La finalul acestei etape se semnează procesul-verbal de recepție cantitativă și de punere în funcțiune.

- Etapa 2 – Predarea documentației finale și instruirea personalului: maximum 5 zile lucrătoare suplimentare după semnarea procesului-verbal de la Etapa 1. La finalul acestei etape se semnează procesul-verbal de recepție finală.

Activitățile cuprinse în termenul total de execuție sunt:

- Livrarea echipamentelor
- Montarea, instalarea și amenajarea (canale cablu, traseu, fixare camere)
- Cablare structurată completă
- Pornirea, configurarea și setarea sistemului
- Integrarea în rețeaua și sistemul de supraveghere existent
- Configurarea regimului de sistem închis
- Testarea funcțională în prezența beneficiarului
- Instruirea personalului desemnat (minim 2 ore) și predarea documentației

Documentație finală: după finalizarea lucrării se va preda beneficiarului un dosar tehnic complet, în 2 exemplare originale + format electronic, cuprinzând:

- Scheme și schițe cu dispunerea și amplasarea echipamentelor și a conexiunilor între ele
- Schema logică de rețea (IP, VLAN, porturi)
- Inventar echipamente (model, serie, MAC, IP, locație)
- Manuale de utilizare și administrare în limba română (pe suport electronic)
- Declarații de conformitate, certificate de garanție
- Lista conturilor configurate (fără parole) și politica de parole aplicată
- Lista funcțiilor cloud / externe dezactivate
- Proces-verbal de instruire utilizatori, semnat de participanți

Lucrările vor fi efectuate organizat, fără afectarea continuității actului medical, astfel încât activitatea la nivelul întregului Institut să se poată desfășura în condiții optime.

Program de lucru: lucrările de instalare, montaj, cablare și orice activitate care poate genera zgomot, praf sau care necesită prezența personalului tehnic în zonele de tratament se vor efectua EXCLUSIV după ora 15:00, în zilele lucrătoare. Acest program este obligatoriu pentru a nu împiedica desfășurarea activității medicale curente. Excepțiile (de exemplu, configurări software sau testări care nu afectează spațiul medical) se pot efectua și în alte intervale orare, doar cu acordul prealabil scris al Serviciului Tehnic și al șefului secției respective.

7. Termen de plată

Plata se va face în termen de 60 de zile de la emiterea facturii, după semnarea procesului-verbal de recepție finală fără obiecțiuni. Plata va fi realizată după alocarea fondurilor necesare de către autoritatea contractantă și în conformitate cu procedurile contabile și legislative aplicabile.

8. Recepție

Recepția lucrării se va efectua în două etape:

a) Recepția cantitativă și de punere în funcțiune (Etapa 1) – se efectuează la finalul Etapei 1 (max. 10 zile lucrătoare), pe baza:

- Verificării livrării tuturor echipamentelor și materialelor conform devizului confirmat de Serviciul Tehnic
- Facturii, declarației de conformitate, certificatelor de garanție
- Testării funcționale a tuturor camerelor, înregistrării, accesului centralizat, alarmelor și privacy mask-urilor
- Verificării integrării în rețeaua locală și în sistemul de supraveghere centralizat
- Bifării checklist-ului pentru regimul de sistem închis

b) Recepția finală (Etapa 2) – se efectuează după predarea integrală a documentației și a instruirii personalului (max. 5 zile lucrătoare suplimentare după recepția Etapei 1), și NUMAI dacă:

- Documentația tehnică completă a fost predată în 2 exemplare originale + format electronic, conform listei de la pct. 6
- Instruirea personalului a fost efectuată și consemnată în proces-verbal semnat de participanți
- Nu sunt identificate neconformități față de cerințele caietului de sarcini

Recepția finală se face doar dacă sistemele funcționează conform cerințelor și nu sunt identificate neconformități. În caz contrar, se acordă termen pentru remedieri, cu reluarea procesului de recepție.

9. Clauze contractuale în mod expres

- Penalități de întârziere: 0,1% / zi de întârziere din valoarea fără TVA a contractului, aplicabile pentru depășirea oricăruia dintre cele două termene de execuție prevăzute la pct. 6 (Etapa 1 – instalare și punere în funcțiune; Etapa 2 – predarea documentației și instruirea), dar nu mai mult de valoarea contractului
- Confidențialitate totală asupra schemei de rețea, parolelor, configurațiilor și a oricăror informații tehnice ale Institutului obținute pe parcursul execuției
- Prestatorul va semna acord de confidențialitate / GDPR cu beneficiarul, în calitate de persoană împuternicită punctual pe durata lucrării

10. Alte mențiuni sau obligații furnizor / prestator / executant

- Personalul executantului care intră în zonele medicale (Lab. Angiografie, Electrofiziologie) va respecta normele de igienă, echipare și circulație ale Institutului
- Toate deșeurile rezultate (resturi cablu, ambalaje, materiale) vor fi evacuate de executant la finalul fiecărei zile de lucru
- Suprafețele, finisajele și echipamentele existente vor fi protejate; eventualele deteriorări vor fi remediate pe cheltuiala executantului
- Executantul va deține autorizație IGPR pentru instalare sisteme de securitate (Legea nr. 333/2003) – copie după licență se va anexa la ofertă
- Operatorii care intervin pe partea de configurare rețea / IT vor avea minim certificare de bază pe echipamentele ofertate (atestat producător sau echivalent)

11. Clauza de revizuire / modificare contractuală

Modificarea contractului pe perioada de execuție este permisă numai în condițiile și limitele prevăzute de legislația aplicabilă în domeniul achizițiilor publice, fără alterarea obiectului contractului și fără afectarea principiilor concurențiale.

12. Subcontractare, integritate și conflict de interese

Ofertantul va respecta obligațiile privind integritatea, evitarea conflictului de interese și conduita etică în derularea procedurii și a contractului.

Ofertantul va declara partea / părțile din contract pe care intenționează să le subcontracteze, dacă este cazul, în condițiile documentației de atribuire și ale legislației aplicabile.

13. Cerințe privind securitatea informațiilor și protecția datelor

Operatorul economic va implementa măsuri tehnice și organizaționale adecvate, astfel încât operarea sistemului să se realizeze în conformitate cu obligațiile legale aplicabile beneficiarului.

Sistemul ofertat va respecta cerințele aplicabile privind securitatea cibernetică și protecția datelor cu caracter personal, inclusiv prin măsuri de control al accesului, jurnalizare, trasabilitate, criptare a comunicațiilor și politici de retenție / configurare a arhivelor.

14. Condiții minime contractuale de execuție

Contractantul va asigura: livrare, instalare, configurare, integrare, testare, punere în funcțiune și instruirea personalului desemnat de beneficiar, în termenul asumat prin ofertă.

La recepție, contractantul va preda în mod obligatoriu: documentația tehnică finală, schema de principiu / as-built, licențele, credențialele de administrare predate în regim controlat, procese-verbale de testare și punere în funcțiune.

Garanția minimă este cea prevăzută în caietul de sarcini, cu obligația asigurării remedierii defecțiunilor în perioada de garanție, conform termenelor asumate contractual.

15. Criteriul de atribuire și evaluarea ofertelor

Criteriul de atribuire rămâne „prețul cel mai scăzut", aplicat exclusiv ofertelor declarate admisibile și conforme tehnic cu toate cerințele minime obligatorii prevăzute în prezentul caiet de sarcini.

Lipsa demonstrării uneia sau mai multor cerințe minime obligatorii conduce la declararea ofertei ca neconformă, în condițiile legii.

16. Demonstrarea conformității și echivalențe

Cerințele tehnice sunt minime și obligatorii, formulate funcțional, fără a restrânge concurența. Orice trimitere la standarde, mărci, procedee, certificări sau origine se consideră însoțită de mențiunea „sau echivalent".

În cazul propunerii unei soluții echivalente, ofertantul are obligația de a demonstra, documentat, că performanțele tehnice, funcționale, de securitate și interoperabilitate sunt cel puțin la nivelul cerințelor minime din caietul de sarcini.

Documentele acceptate pentru demonstrarea conformității includ, fără a se limita la: fișe tehnice oficiale ale producătorului, declarații de conformitate, certificate de produs / sistem, rapoarte de testare, manuale tehnice și documentație oficială de integrare.

Ofertantul va prezenta, în mod obligatoriu, matricea de conformitate cerință – răspuns, cu indicarea explicită a documentului justificativ și a paginii relevante pentru fiecare cerință minimă.

17. Fișe tehnice

Fișele tehnice (1 – Platformă software unificată, 2 – Camere video interior, 3 – Server video, 4 – Licență interconectare camere) sunt prezentate în Anexa de la finalul prezentului document și fac parte integrantă din caietul de sarcini.

Șef Serviciu Administrativ ec. Sălăjan Lenuța	**Întocmit,** ec. Mihalca Ana-Maria

ANEXĂ LA CAIETUL DE SARCINI

FIȘE TEHNICE

Fișele tehnice de mai jos detaliază cerințele minime obligatorii pentru fiecare componentă a sistemului. Ofertantul va completa coloanele „Corespondență ofertă" și „Document justificativ / Observații", indicând explicit modul în care soluția propusă îndeplinește fiecare cerință și documentul/pagina relevantă din oferta tehnică.

Fișa tehnică nr. 1

Platforma unificată de securitate

1. Parametri tehnici și funcționali

1.1. Cerințe generale platformă unificată

- Sistemul de securitate va face parte dintr-o platformă unificată de securitate atotcuprinzătoare, care va sprijini integrarea perfectă a sistemului automat de recunoaștere a plăcuțelor de înmatriculare IP (ALPR), a sistemului de control al accesului IP și a sistemului de gestionare video IP (VMS) sub un singur software.
- Producătorul trebuie să garanteze că soluția software face parte din linia oficială de produse a producătorului, concepute pentru utilizare comercială și/sau industrială pe tot parcursul anului (24/7/365), cu experiență similară dovedită de cel puțin 20 ani.
- Trebuie să prezinte o interfață de securitate unificată pentru gestionarea, configurarea, monitorizarea și raportarea sistemelor ALPR, sistemului de control al accesului și VMS încorporate și a dispozitivelor edge asociate.
- Platforma va putea fi configurată în așa fel încât componentele de control al accesului să fie conforme cu standardele stricte Grad 4, conform EN 60839-11-1.
- Trebuie să aibă capacitatea de a crea și personaliza tablouri de bord dinamice live pentru monitorizarea sistemului, permițând date precum: diagnostice de sănătate și rapoarte cu reprezentarea grafică a acestor date, rapoarte SDK, informații meteo, video live, evenimente de control acces, alarme, punctaj de securitate cibernetică printr-un ghid de întărire încorporat.
- Să permită actualizarea driverelor camerelor sale independent de instalare.
- Arhitectură deschisă, care permite utilizarea de stații de lucru, servere, infrastructuri de rețea și echipamente de stocare non-proprietar.
- Soluție completă și scalabilă de supraveghere video, cu posibilitatea adăugării camerelor în sistem bucată cu bucată.
- Trebuie să fie compatibilă cu DVS (servere video digitale) de la diverși producători (encodere video analog-digitale, camere IP, decodoare video digital-analogice).
- Toate fluxurile video și audio furnizate de camere analogice sau de camere IP trebuie să fie codificate digital și înregistrate simultan în timp real.
- Să permită configurarea unui fus orar pentru fiecare cameră conectată la un DVS (posibilitatea de a căuta videoclipuri pe baza orei locale, GMT, alt fus orar etc.).
- În sistemul global de stocare trebuie să fie posibilă includerea discurilor amplasate pe NAS, PC-uri etc. (din LAN/WAN).

1.2. Securitate cibernetică

- Platforma unică de securitate trebuie să fie o soluție bazată pe comunicație IP. Toate comunicațiile dintre server și aplicația client să se bazeze pe protocolul TCP/IP standard și să utilizeze criptarea și certificate digitale pentru a securiza canalul de comunicare.

- Trebuie să aibă posibilitatea de a cripta fluxul media, inclusiv video, audio și metadate, în repaus și în tranzit.
- Trebuie să permită setarea criptării per cameră, iar când aceasta este activă, performanța de înregistrare nu va fi redusă peste 50%.
- Trebuie să utilizeze o cheie de criptare aleatorie care va fi schimbată periodic.
- Trebuie să suporte criptarea pentru toate comunicațiile cu bazele sale de date.
- Va sprijini autentificarea pasivă utilizând OpenID Connect și SAML 2.0.
- Certificare CSPN de la ANSSI (opțional) – certificarea demonstrează robustețea produselor, pe baza unei analize de conformitate și a unor teste de penetrare efectuate de un evaluator terț sub autoritatea unei agenții de Securitate cibernetică Europene, recunoscută internațional.
- Certificare UL 2900-2-3 Nivelul 3 de pregătire pentru securitatea cibernetică – emisă de o organizație recunoscută internațional, ce colaborează cu Departamentul pentru Securitate Internă din SUA pentru securitatea IoT.
- Standardul ISO/IEC 27001 – standard de securitate a informațiilor; specifică cele mai bune practici pentru un sistem de management al securității informațiilor (ISMS).

1.3. Certificare DHS Safety Act

- Platforma este calificată de către Departamentul de Securitate internă al unui stat NATO ca fiind o tehnologie anti-terorism, eficientă în facilitarea apărării împotriva actelor de terorism, inclusiv pentru prevenirea, învingerea sau a oferi răspuns la astfel de acte.
- Datorită criteriului de sensibilitate al instalării, platforma va fi calificată anti-terorism și certificată ca produs aprobat pentru securitatea internă de la o instituție relevantă precum Departamentul de Securitate Internă al Statelor Unite (DHS) sau similar.
- Va fi o soluție bazată pe IP. Toate comunicările se bazează pe protocolul TCP/IP standard și utilizează criptarea TLS cu certificate digitale pentru securizarea canalului de comunicare.
- Va sprijini autentificarea utilizatorilor cu autentificarea bazată pe revendicări folosind furnizori externi.
- Sistemul trebuie să poată schimba starea întregii platforme de securitate (LPR, video, control acces, interfoane SIP etc.) pe baza oricărui eveniment. Activarea nivelului de amenințare trebuie să poată iniția partajarea entităților (video, LPR, acces etc.) către o întreprindere separată care nu are legătură cu întreprinderea inițiatoare.

1.4. Arhivarea

- Trebuie să utilizeze o bază de date cu evenimente și marcaje temporale pentru căutarea avansată a arhivelor audio/video.
- Trebuie să semneze digital înregistrările video utilizând un algoritm de semnătură bazat pe o criptografie cu cheie publică/privată.

- Trebuie să aibă opțiune de prealarmă și de înregistrare după alarmă care poate fi setată între o secundă și cinci minute per cameră.
- Trebuie să aibă funcționalitatea de stocare a fluxurilor video și audio pe baza declanșării (exemplu: detectare mișcare).
- Trebuie să detecteze mișcarea video în decurs de maxim 250 de milisecunde și nu numai pe cadrele cheie.
- Trebuie să permită alocarea mai multor programe de înregistrare unei singure camere în funcție de modul de înregistrare (continuu, manual etc.) și recurență (zilnic, săptămânal etc.).
- Administratorul trebuie să aibă opțiuni de gestionare a discului: să aleagă ce discuri să utilizeze pentru arhivare, să stabilească o cotă maximă pentru fiecare, să răspândească arhivarea diferitelor camere pe diferite grupuri de discuri.
- Trebuie să aibă posibilitatea de curățare a arhivelor vechi, pentru fiecare cameră în parte (după un număr de zile, oprire automată dacă discurile sunt pline, ștergerea în mod prioritar a arhivelor vechi etc.).
- Trebuie să aibă posibilitatea de eșantionare a fluxurilor video în scopuri de economisire a spațiului de stocare.
- Trebuie să suporte înregistrarea locală în server și să ofere posibilitatea de redare a videoclipurilor înregistrate pe server la viteze diferite.
- Trebuie să poată descărca imaginile video înregistrate pe server după program, în funcție de eveniment, sau manual pentru a le arhiva, utilizând diverse filtre.
- Trebuie să aibă posibilitatea de a cripta fluxul media provenit din server, inclusiv video, audio și metadate în repaus și în tranzit.

1.5. Streaming media VMS și transfer arhive video

- Routerul media trebuie să fie responsabil pentru direcționarea fluxurilor video și audio prin rețelele locale și extinse de la sursă la destinație.
- Routerul media trebuie să suporte mai multe protocoale de transport unicast TCP, unicast și multicast.
- Routerul media trebuie să utilizeze agenți de redirecționare și este responsabil pentru redirecționarea unui flux de la o sursă IP la o destinație IP.
- Trebuie să fie posibilă limitarea numărului de redirecționări video simultane în timp real pentru a controla mai bine lățimea de bandă.
- Trebuie să aibă capacitatea de a transfera video de la memoria camerei la un server, de pe un server/server federalizat pe un alt server din același sistem.
- Trebuie să aibă posibilitatea de filtrare a videoclipurilor de interes pentru un transfer.
- Trebuie să fie posibilă definirea lungimii videoclipului înainte și după evenimentul utilizat ca filtru pentru a determina videoclipul de interes.

1.6. Cerințele generale ale software-ului client

- Trebuie să furnizeze interfața cu utilizatorul pentru configurarea și monitorizarea platformei de securitate în orice rețea și să fie accesibilă local sau printr-o conexiune la distanță.
- Trebuie să aibă interfață de utilizare pentru configurarea sistemului și pentru monitorizare, bazată pe Windows, cu interfață grafică ușor de utilizat.
- Trebuie să îmbine recunoașterea plăcuțelor de înmatriculare (LPR) și funcționalitățile video în cadrul aceleiași aplicații de utilizator.
- Toate aplicațiile trebuie să ofere un mecanism de autentificare care verifică valabilitatea utilizatorului.
- Administratorul (care are toate drepturile și privilegiile) trebuie să poată defini drepturi de acces și privilegii specifice pentru fiecare utilizator din sistem.
- Configurația tuturor sistemelor VMS și LPR încorporate trebuie să fie accesibilă prin intermediul interfeței de utilizare pentru configurare.
- Trebuie să includă o varietate de instrumente, cum ar fi utilitare de depanare, instrumente de import și un instrument de descoperire a echipamentelor.
- Trebuie să îndeplinească rolul unei interfețe de securitate unificate care este capabilă să monitorizeze evenimentele și alarmele video și LPR, precum și să vizualizeze video în timp real și înregistrat.

1.7. Interfață utilizator client VMS – monitorizare

- Monitorizarea trebuie să aibă unul sau mai multe dintre următoarele elemente: listă de evenimente, arbore logic (camerele, zonele, unitățile LPR grupate în arii ierarhic), lista tuturor entităților urmărite.
- Trebuie să aibă posibilitatea de personalizare a spațiului de lucru al utilizatorului printr-o varietate de opțiuni de personalizare selectabile (limitate de administrator).
- Trebuie să fie în măsură să monitorizeze activitatea camerelor LPR și video, să suporte: monitorizarea evenimentelor live (VMS și/sau LPR); generarea de rapoarte personalizate; monitorizarea și confirmarea alarmelor; crearea și editarea incidentelor; afișarea și executarea acțiunilor direct din hărțile grafice.
- Capacitățile video avansate trebuie să includă: vizualizare video live avansată; redare a arhivelor video; gestionarea evenimentelor și alarmelor; rapoarte video; controlul camerelor PTZ; cereri de transfer arhive; date suprapuse pe video live sau redat.
- Vizualizare live: zoom digital pe transmisii live, rotire-înclinare, focalizare, pornire/oprire, poze, redare audio și video pentru orice interval de timp.
- Trebuie să aibă capacitatea de a controla redarea: pauză, viteză, redare cadru cu cadru, redare 1/4x, 1/2x, 1x, 2x, 4x, 6x, 8x etc.
- Trebuie să aibă posibilitatea de a afișa o singură cronologie sau o cronologie pentru fiecare flux video selectat, nivelul de mișcare în orice punct și evenimentele marcate.

- Trebuie să aibă capacitatea de a defini o zonă a câmpului video în care să se caute mișcare și cantitatea de mișcare care va furniza rezultatele căutării.
- Trebuie să aibă instrumente pentru exportul de conținut video și player video autonom pe diferite suporturi.
- Pentru LPR: monitorizarea și gestionarea evenimentelor și alarmelor LPR; vizualizarea imaginilor plăcuțelor de înmatriculare și a imaginilor de context; verificarea datelor LPR cu video live și înregistrate.
- Pentru LPR: selectarea mai multor regiuni pe o hartă; protejarea unei citiri sau a unui rezultat pozitiv împotriva ștergerii; crearea unei liste de interes; urmărirea poziției patrulei; raport de citiri pozitive; vizualizare pe hartă; căutarea numerelor de înmatriculare complete sau parțiale.

1.8. Platforma de securitate – arhitectură

- Trebuie să se bazeze pe un model client/server, format dintr-un modul software server standard și aplicații software client.
- Soluție bazată pe tehnologie IP. Toate comunicațiile dintre server și client se bazează pe TCP/IP standard și utilizează criptarea cu certificate digitale.
- Modulul server trebuie să fie un serviciu Windows care poate fi configurat să pornească odată cu sistemul de operare și să ruleze în fundal, indiferent dacă un utilizator este sau nu conectat.
- Numărul de module software server trebuie să nu fie limitat.
- Trebuie să suporte conceptul de Federare prin care mai multe instanțe independente (video management, LPR) pot fi fuzionate într-un singur sistem virtual mare pentru monitorizare centralizată, raportare și gestionare.
- Trebuie să suporte număr nelimitat de aplicații software client (cel puțin 100 conectate simultan).
- Trebuie să fie o arhitectură bazată pe roluri, fiecare rol fiind definit pentru un set de sarcini dintr-un subsistem.
- Trebuie să aibă monitorizare și control de la distanță al conținutului altor stații de lucru care rulează software tip client.
- Administratorul trebuie să fie capabil să atribuie sarcini și să blocheze spațiul de lucru al operatorului. Gestionarea spațiului de lucru de către utilizatori este limitată de privilegiile atribuite.
- Trebuie să faciliteze generarea de rapoarte pentru sistemul video și LPR: alarmă, specifice video, LPR, statistici, audit, incidente etc.
- Trebuie să aibă capacitatea de a crea tablouri de bord cu permisiuni de vizualizare pe bază de privilegii acordate în prealabil.
- Trebuie să permită configurarea și gestionarea utilizatorilor și a grupurilor de utilizatori. Drepturile și privilegiile de acces comune partajate de mai mulți utilizatori trebuie să fie definite ca grupuri de utilizatori.

- Trebuie să fie posibilă specificarea privilegiilor pentru fiecare partiție; opțiuni avansate de autentificare, cum ar fi autentificarea cu supervizare.
- Trebuie să permită utilizatorilor să automatizeze și să extindă funcționalitățile sistemului prin macro comenzi sau scripturi personalizate pentru controlul accesului, video și LPR.
- Trebuie să furnizeze o interfață centrată pe hartă cu capacitatea de a comanda și controla toate capabilitățile platformei dintr-o interfață de hartă cu ecran complet.

1.9. Integrarea platformei de securitate cu sistemul video și LPR

- Interfața utilizatorului de monitorizare trebuie să prezinte o interfață integrată și securizată pentru monitorizarea și raportarea în timp real a sistemului video și LPR.
- Configurarea trebuie să fie posibilă dintr-o interfață integrată pentru toate sistemele.
- Trebuie să fie posibilă vizualizarea videoclipurilor asociate evenimentelor LPR atunci când se vizualizează un raport.
- Trebuie să suporte diverse funcționalități pentru gestionarea alarmelor: crearea și modificarea, definirea afișării de conținut video, setarea nivelului de prioritate, grupare, automatizare etc.
- Utilizatorul trebuie să aibă capacitatea de a confirma alarmele, de a crea un incident la confirmarea alarmei și de a amâna o alarmă.
- Trebuie să permită importul de date din surse externe pentru a spori unificarea surselor de date.

1.10. Jurnale de audit și de activitate a utilizatorilor

- Trebuie să aibă jurnalele de completări, ștergeri și modificări efectuate de operator/administrator.
- Jurnalele de audit trebuie să fie generate sub formă de rapoarte și să poată urmări modificările efectuate în anumite perioade de timp.
- Trebuie să fie posibilă interogarea cu privire la anumiți utilizatori, anumite modificări, entitățile afectate și perioadele de timp.
- Trebuie să includă informații detaliate privind valoarea înainte și după modificări.
- Trebuie să permită tipărirea raportului și exportarea raportului într-un fișier PDF / Microsoft Excel / CSV etc.

1.11. Rapoarte de incidente

- Trebuie să permită operatorului de securitate să creeze rapoarte privind incidentele care au avut loc într-un interval de timp.
- Trebuie să poată crea rapoarte de incidente independente sau rapoarte de incidente legate de alarme.
- Trebuie să poată conecta mai multe secvențe video la un incident, să le acceseze într-un raport și să modifice data sau ora secvențelor ulterior.

- Trebuie să permită crearea unui formular personalizat pe baza căruia să se introducă informații privind un incident.

1.12. Integrare cu alte aplicații

- Trebuie să sprijine abordări multiple pentru integrarea sistemelor terțe: kituri de dezvoltare software (SDK-uri), SDK-uri de servicii web bazate pe REST, SDK-uri de servicii RTSP.
- Arhitectura sistemului va sprijini adăugarea de noi conectori în sistem pentru integrarea cu terți: analiză video, sisteme video terțe, sisteme de control al accesului terțe, sisteme de management al clădirilor, IoT industrial (Modbus, BACnet, OPC, SNMP, http Server, MQTT Client, TCP Server), Videowall, sisteme HRMS, integrarea autonomă a dronelor.
- Sistemul trebuie să poată importa date din surse externe și să definească tipuri de date particularizate ca orice combinație de șiruri, numere, marcaje temporale, imagini și componente. Datele trebuie să poată fi importate printr-un fișier, introduse manual pe o hartă sau prin altă metodă aprobată. Datele ingerate trebuie să poată declanșa evenimente, efectua analize de corelare și să fie afișate pe hărți și tablouri de bord.

2. Specificații de performanță și condiții privind exploatarea

Sistemul va asigura funcționare continuă 24/7/365, cu capacitate de scalare incrementală și fără degradarea performanței la adăugarea de noi camere sau utilizatori.

3. Condiții de garanție

Garanție minimă: 48 de luni pentru platforma software.

4. Alte condiții

Toate licențele software vor fi predate beneficiarului în original, pe numele Institutului Inimii de Urgență pentru Boli Cardiovasculare „Niculae Stăncioiu" Cluj-Napoca.

Fișa tehnică nr. 2

Camere supraveghere video color IP – interior

Cerințe minime tehnice pentru cele 10 camere de supraveghere video care vor fi instalate în Lab. Angiografie (3 camere), Compartiment Electrofiziologie (2 camere) și sala de așteptare Ambulator parter (5 camere).

Specificație	Performanță / Valoare solicitată	Corespondență ofertă	Document justificativ / Observații
Model cameră	Dome		
Tip cameră	5MP AI IR Micro Vandal Dome Camera		
Rezoluție maximă	5MP (2592 x 1944)		
Senzor imagine	1/2.8"		
Framerate maxim	30 fps / 25 fps (60Hz / 50Hz)		
Iluminare minimă color	0.03 lux		
Iluminare minimă BW	0.003 lux		
Lentilă	3 mm fixă		
Diafragmă maximă	F1.6		
Unghi vizualizare orizontal	100°		
Unghi vizualizare vertical	73°		
Unghi vizualizare diagonal	129°		
Distanță minimă obiect	0.55 m		
Day & Night	Auto (ICR)		
Reducere zgomot digital	WiseNR II (AI engine), SSNRV		
Detecție mișcare	Da (8 zone)		
Mascare intimitate	Da (32 zone)		
Iluminator IR	LED IR, 20 m, 850 nm		

Specificație	Performanță / Valoare solicitată	Corespondență ofertă	Document justificativ / Observații
Analitice AI	Detecție obiecte (persoană/vehicul), linie virtuală, zonă virtuală, mișcare		
Business intelligence	People counting, Queue management, Heatmap, Vehicle counting		
Compresie video	H.265 / H.264 / MJPEG		
Streaming	Până la 5 profile, unicast/multicast, până la 20 utilizatori		
Rețea Ethernet	RJ-45 (10/100BASE-T)		
Protocoale relevante	IPv4/IPv6, RTSP, HTTPS, SNMP, MQTT, SRTP, ONVIF S/G/T/M		
Stocare locală	MicroSD/SDHC/SDXC, max. 256 GB		
Memorie	RAM 2 GB, Flash 1 GB		
Alimentare	PoE (IEEE 802.3af, Class 3)		
Consum	Max. 8.7 W, tipic 5 W		
Temperatură operare	-39°C ÷ +53°C		
Umiditate operare	0 ÷ 100% RH (condensing)		
Grad protecție	IP66		
Rezistență antivandal	IK10		
Certificare mediu	NEMA 4X		

Camerele vor fi compatibile nativ cu platforma unificată descrisă în Fișa tehnică nr. 1 și cu serverul video descris în Fișa tehnică nr. 3.

Fișa tehnică nr. 3

Server video

Cerințe minime tehnice pentru serverul video care va găzdui platforma de management și înregistrările provenite de la cele 10 camere IP.

Specificație	Performanță / Valoare solicitată	Corespondență ofertă	Document justificativ / Observații
Model / serie echipament	Server		
Capacitate stocare brută	25 TB RAW scalabil		
Procesor	Xeon		
Memorie RAM	32 GB RAM		
Stocare sistem	2 x 480 GB		
Stocare date	4 x 6 TB HDD		
Interfețe rețea 1GbE	1 x 1GbE RJ45		
Sursă alimentare	1 x 900W PSU		
Sistem de operare	Windows 11 Professional		
Garanție	2 ani next business day		
Software preinstalat	Software platformă VMS conform Fișa tehnică nr. 1 preinstalled		
Licențiere	Licență Windows 11 Pro		

Serverul va fi livrat cu software platformă VMS conform Fișa tehnică nr. 1 preinstalat și configurat. Toate licențele și mediile de instalare vor fi predate beneficiarului. Serverul va fi integrat în domeniul / VLAN-ul de supraveghere video al Institutului, fără acces direct la internet, conform regimului de sistem închis prevăzut în caietul de sarcini.

Fișa tehnică nr. 4

Licență interconectare camere video la platforma integrată

Cerințe minime pentru licențele software per cameră IP, necesare interconectării celor 10 camere video la serverul VMS / platforma unificată de securitate.

Cerință minimă	Răspuns ofertat	Dovadă
Licență software per cameră IP pentru interconectare la serverul VMS	Se oferă licență per cameră IP (1 licență/cameră)	Fișă tehnică produs + listă licențe ofertate
Licența permite înrolarea/autorizarea camerei în serverul de management/arhivare	Conform	Documentație producător (capitol Add/Enroll Camera)
Vizualizare live și playback pentru camera licențiată	Conform	Manual utilizare client VMS
Înregistrare continuă, la eveniment și după program (schedule)	Conform	Fișă funcțională VMS + capturi configurare
Suport flux principal/secundar (main/sub stream), configurare codec și bitrate	Conform	Datasheet VMS / ghid configurare video
Suport evenimente/alarme cameră și metadate asociate	Conform	Documentație integrare cameră + listă evenimente
Management drepturi utilizator pe cameră/flux (roluri/permisiuni)	Conform	Manual administrare utilizatori
Compatibilitate cu arhitectura client-server și scalare incrementală (adăugare camere în etape)	Conform	Arhitectură soluție + fișă scalabilitate
Compatibilitate ONVIF Profile S/G/T (sau echivalent) pentru integrare multi-vendor	Conform	Declarație compatibilitate / certificat ONVIF
Licență perpetuă sau pe termen definit, cu condițiile de suport/upgrade clar precizate	Se precizează tipul licenței și perioada suportului	Ofertă comercială + termeni licențiere

Cantitatea ofertată va fi de minim 10 licențe (1 licență/cameră), corespunzătoare numărului de camere prevăzute în prezenta documentație. Ofertantul va preciza explicit tipul licenței (perpetuă sau pe termen definit), perioada de suport inclusă și condițiile de upgrade.