CONTRACT Nr. _69_
privind achiziţia de bunuri

I PARTEA GENERALĂ

Obiectul achiziţiei: **Implementarea Platformei Integrate de Monitorizare**

Cod CPV: 48200000-0

" 21 " august 2025 *mun. Chişinău*

Furnizorul de bunuri	Autoritatea contractantă
SC "RAPID LINK" SRL reprezentat prin administrator **Victor BACIU**, care acţionează în baza **Statutului**, c/f 1007600035161, denumit în continuare ***Furnizor,*** pe de o parte,	**Serviciul Tehnologii Informationale al MAI** reprezentat prin director **Ion BOTNARI**, care acţionează în baza **Regulamentului**, c/f 1013601000521, denumit în continuare ***Cumpărător***, pe de altă parte,

ambii denumiţi în continuare Părţi, au încheiat prezentul Contract referitor la următoarele:

a. Achiziţionarea şi implementarea ***Platformei Integrate de Monitorizare***, denumite în continuare Bunuri, conform procedurii de achiziţii publice de tip licitaţie deschisă nr. MD-1750325094164 din 19.06.2025, în baza deciziei grupului de lucru al Beneficiarului din 30 iulie 2025.

b. Următoarele documente vor fi considerate părţi componente ale Contractului:
- Specificaţia tehnică, Anexa nr. 1;
- Specificaţia de preţ, Anexa nr. 2;
- Caiet de sarcini, Anexa nr. 3.

c. În cazul unor discrepanţe sau inconsecvenţe între documentele componente ale Contractului, documentele vor avea ordinea de prioritate enumerată mai sus.

d. În calitate de contravaloare a plăţilor care urmează a fi efectuate de Cumpărător, Furnizorul se obligă prin prezentul contract să livreze Cumpărătorului Bunurile şi să înlăture defectele lor în conformitate cu prevederile Contractului sub toate aspectele.

e. Cumpărătorul se obligă prin prezentul contract să plătească Furnizorului, în calitate de contravaloare a livrării bunurilor, preţul Contractului în termenele şi modalitatea stabilite de Contract.

1. OBIECTUL CONTRACTULUI

1.1. Furnizorul îşi asumă obligaţia de a livra Bunurile, conform Specificaţiilor *(Anexa nr. 1; Anexa nr. 2 şi Anexa nr. 3)*, care este parte integrantă a prezentului Contract.

1.2. Cumpărătorul se obligă, la rândul său, să achite şi să recepţioneze Bunurile livrate de Furnizor.

1.3. Calitatea Bunurilor se atestă prin certificatele de calitate indicate în Specificaţie.

1.4. Bunurile livrate în baza contractului vor respecta standardele indicate în Specificaţia tehnică.

1.5. Termenul de garanţie a Bunurilor este de **3 (trei) ani** din data acceptanţei finale.

2. TERMENI ŞI CONDIŢII DE LIVRARE

2.1. Livrarea Bunurilor se efectuează de către Furnizor până la 60 de zile de la inregistrarea la Ministerul Finanţelor.

2.2. Documentaţia de însoţire a Bunurilor include:

a) Factura fiscală electronică (e – factură);

b) Actul de acceptanţă finală a bunurilor agreat de ambele părţi;

c) Documentaţia tehnică GENETEC Security Center; Irisity Iris; VaxALPR;

d) Actul de instruire utilizatori și administratori;

d) Certificat de garanție pentru bunurile livrate.

2.3. Originalele documentelor prevăzute în punctul 2.2. se vor prezenta Cumpărătorului cel târziu la momentul livrării bunurilor la destinația finală. Livrarea bunurilor se consideră încheiată în momentul în care sunt prezentate documentele de mai sus.

3. PREȚUL ȘI CONDIȚII DE PLATĂ

3.1. Prețul Bunurilor livrate conform prezentului Contract este stabilit în lei MD, fiind indicat Specificația prezentului Contract.

3.2. Suma totală a prezentului Contract, inclusiv TVA, se stabilește în lei MD și constituie: **7 260 000,00 (șapte milioane două sute șasezeci mii lei 00 bani) MD.**

3.3. Achitarea plăților pentru Bunurile livrate se va efectua în lei MD.

3.4. Metoda și condițiile de plată de către Cumpărător vor fi*: **achitarea va fi efectuată după livrarea bunurilor și semnarea actului de acceptanță finală în termen de până la 15 zile calendaristice, în baza facturii fiscale electronice (e-factură) și actelor, semnate de ambele Părți, în corespundere cu volumul bunurilor livrate.***

3.5. Plățile se vor efectua prin transfer bancar pe contul de decontare al Furnizorului indicat în prezentul Contract.

4. CONDIȚII DE PREDARE-PRIMIRE

4.1. Bunurile se consideră predate de către Furnizor și recepționate de către Cumpărător dacă:

a) cantitatea Bunurilor corespunde informației indicate în Specificații *(Anexa nr.1, nr.2 și nr.3)* și documentelor de însoțire conform punctului 2.2. al prezentului Contract;

b) calitatea Bunurilor corespunde informației indicate în Specificații *(Anexa nr.1, nr.2 și nr.3)*;

c) ambalajul și integritatea Bunurilor corespunde informației indicate în Specificații.

4.2. Furnizorul este obligat să prezinte Cumpărătorului un exemplar original al facturii fiscale odată cu livrarea Bunurilor, pentru efectuarea plății. Pentru nerespectarea de către Furnizor a prezentei clauze, Cumpărătorul își rezervă dreptul de a majora termenul de achitare prevăzut în punctul 3.4. corespunzător numărului de zile de întârziere și de a fi exonerat de achitarea penalității stabilite în punctul 10.4.

5. STANDARDE

5.1. Bunurile livrate în baza contractului vor respecta standardele prezentate de către furnizor în propunerea sa tehnică.

5.2. Când nu este menționat nici un standard sau reglementare aplicabilă se vor respecta standardele sau alte reglementări autorizate în țara de origine a Bunurilor.

6. OBLIGAȚIILE PĂRȚILOR

6.1. În baza prezentului Contract, Furnizorul se obligă:

a) să livreze Bunurile în condițiile prevăzute de prezentul Contract;

b) să anunțe Cumpărătorul după semnarea prezentului Contract, în decurs de 2 zile calendaristice, prin telefon/fax sau mijloace electronice, despre disponibilitatea livrării Bunurilor;

c) să asigure condițiile corespunzătoare pentru recepționarea Bunurilor de către Cumpărător, în termenele stabilite, în corespundere cu cerințele prezentului Contract;

d) să asigure integritatea și calitatea Bunurilor pe toată perioada de până la recepționarea lor de către Cumpărător.

6.2. În baza prezentului Contract, Cumpărătorul se obligă:

a) să întreprindă toate măsurile necesare pentru asigurarea recepționării în termenul stabilit a Bunurilor livrate în corespundere cu cerințele prezentului Contract;

b) să asigure achitarea Bunurilor livrate, respectând modalitățile și termenele indicate în prezentul Contract.

7. CIRCUMSTANȚE CARE JUSTIFICĂ NEEXECUTAREA CONTRACTULUI

7.1. Părțile sunt exonerate de răspundere pentru neîndeplinirea parțială sau integrală a obligațiilor conform prezentului Contract, dacă aceasta este cauzată de producerea unor cazuri de circumstanțe care

justifică neexecutarea contractului (războaie, calamităţi naturale: incendii, inundaţii, cutremure de pământ, precum şi alte circumstanţe care nu depind de voinţa Părţilor).

7.2. Partea care invocă clauza circumstanţelor care justifică neexecutarea contractului este obligată să informeze imediat (dar nu mai tîrziu de 10 zile) cealaltă Parte despre survenirea circumstanţelor care justifică neexecutarea contractului.

7.3. Survenirea circumstanţelor care justifică neexecutarea contractului, momentul declanşării şi termenul de acţiune trebuie să fie confirmate printr-un aviz de atestare, eliberat în mod corespunzător de către organul competent din ţara Părţii care invocă asemenea circumstanţe.

7.4. În cazul în care în circumstanţele care justifică neexecutarea contractului, acesta se modifică prin acordul adiţional, inclusiv modificarea termenilor de executare, în cazul unei executări ulterioare a contractului. Când se execută pct. 7.1 şi pct. 7.3, părţile modifică contractul prin acord - adiţional, privind neîndeplinerea parţială sau integrală a obligaţiunilor, inclusiv modificarea termenilor în cazul suspendării şi executării ulterioare a contractului.

8. REZOLUŢIUNEA

8.1. Rezoluţiunea Contractului se poate realiza cu acordul comun al Părţilor.

8.2. Contractul poate fi rezolvit în mod unilateral de către:

a) Cumpărător în caz de refuz al Furnizorului de a livra Bunurile prevăzute în prezentul Contract;

b) Cumpărător în caz de nerespectare de către Furnizor a termenelor de livrare stabilite;

c) Furnizor în caz de nerespectare de către Cumpărător a termenelor de plată a Bunurilor;

d) Furnizor sau Cumpărător în caz de nesatisfacere de către una dintre Părţi a pretenţiilor înaintate conform prezentului Contract.

8.3. Cumpărător are dreptul de a rezolvi unilateral contractul în perioada de valabilitate a acestuia în una dintre următoarele situaţii:

a) contractantul se afla, la momentul atribuirii lui, în una dintre situaţiile care ar fi determinat excluderea sa din procedura de atribuire potrivit art. 19 al Legii nr. 131/2015 privind achiziţiile publice;

b) contractul a făcut obiectul unei modificări substanţiale care necesita o nouă procedură de achiziţie publică în conformitate cu art. 76 al Legii nr. 131/2015 privind achiziţiile publice;

c) contractul nu ar fi trebuit să fie atribuit contractantului respectiv, având în vedere o încălcare gravă a obligaţiilor ce rezultă din Legea nr. 131/2015 privind achiziţiile publice şi/sau tratatele internaţionale la care Republica Moldova este parte, care a fost constatată printr-o decizie a unei instanţe judecătoreşti naţionale sau, după caz, internaţionale.

8.4. Partea iniţiatoare a rezoluţiunii Contractului este obligată să comunice în termen de 5 zile lucrătoare celeilalte Părţi despre intenţiile ei printr-o scrisoare motivată.

8.5. Partea înştiinţată este obligată să răspundă în decurs de 5 zile lucrătoare de la primirea notificării. În cazul în care litigiul nu este soluţionat în termenele stabilite, partea iniţiatoare va iniţia rezoluţiunea.

9. RECLAMAŢII

9.1. Reclamaţiile privind cantitatea Bunurilor livrate sunt înaintate Furnizorului la momentul recepţionării lor, fiind confirmate printr-un act întocmit în comun cu reprezentantul Furnizorului.

9.2. Pretenţiile privind calitatea bunurilor livrate sunt înaintate Furnizorului în termen de 5 zile de la depistarea deficienţelor de calitate şi trebuie confirmate printr-un certificat eliberat de o entitate independentă neutră şi autorizată în acest sens.

9.3. Furnizorul este obligat să examineze pretenţiile înaintate în termen de 5 zile de la data primirii acestora şi să comunice Cumpărătorului despre decizia luată.

9.4. În caz de recunoaştere a pretenţiilor, Furnizorul este obligat, în termen de 5 zile, să livreze suplimentar Cumpărătorului cantitatea nelivrată de bunuri, iar în caz de constatare a calităţii necorespunzătoare să le substituie sau să le corecteze în conformitate cu cerinţele Contractului.

9.5. Furnizorul poartă răspundere pentru calitatea Bunurilor în limitele stabilite, inclusiv pentru viciile ascunse.

9.6. În cazul devierii de la calitatea confirmată prin certificatul de calitate întocmit de o entitate independentă neutră sau autorizată în acest sens, cheltuielile pentru staţionare sau întârziere sunt suportate de partea vinovată.

10. SANCȚIUNI

10.1. Forma de garanție de bună executare a contractului agreată de Cumpărător este garanție bancară/transfer bancar la contul Beneficiarului, în cuantum de **5 %** din valoarea contractului.

10.2. Pentru refuzul de a vinde Bunurile prevăzute în prezentul Contract, se va reține garanția de bună executare a contractului, în cazul în care ea a fost constituită în conformitate cu prevederile punctului 10.1. în caz contrar Furnizorul suportă o penalitate în valoare de **5 %** din suma totală a contractului.

10.3. Pentru livrarea cu întârziere a Bunurilor, Furnizorul suportă o penalitate în valoare de **0,1 %** din suma Bunurilor nelivrate, pentru fiecare zi de întârziere, dar nu mai mult de **5 %** din suma totală a prezentului Contract. În cazul în care întârzierea depășește **10 (zece) zile**, Furnizorul prezintă Cumpărătorului o explicație în formă scrisă. Dacă Cumpărătorul acceptă, Furnizorul prelungește termenul de valabilitate a garanției de bună executare, în caz contrar se consideră ca fiind refuz de a livra Bunurile prevăzute în prezentul Contract și Furnizorului i se va reține garanția de bună executare a Contractului, în cazul în care a fost constituită în conformitate cu prevederile pct. 10.1.

10.4. Pentru achitarea cu întârziere, Cumpărătorul suportă o penalitate în valoare de **0,1 %** din suma Bunurilor neachitate, pentru fiecare zi de întârziere, dar nu mai mult de **5 %** din suma totală a prezentului contract.

10.5. Prima zi lucrătoare ulterioară datei ce constituie termenul limită de livrare, precum și, termenul limită de achitare se consideră zi lucrătoare de întârziere.

10.6. Suma penalității calculate Furnizorului conform prezentului Contract poate fi dedusă (reținută) de către Cumpărător din suma plății pentru Bunurile livrate.

11. DREPTURI DE PROPRIETATE INTELECTUALĂ

11.1. Furnizorul are obligația să despăgubească Cumpărătorul împotriva oricăror:

a) reclamații și acțiuni în justiție, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), legate de echipamentele, materialele, instalațiile sau utilajele folosite pentru sau în legătură cu produsele achiziționate;

b) daune-interese, costuri, taxe și cheltuieli de orice natură, aferente, cu excepția situației în care o astfel de încălcare rezultă din respectarea Caietului de sarcini întocmit de către Cumpărătorul.

12. DISPOZIȚII FINALE

12.1. Litigiile din prezentul Contract vor fi soluționate de către Părți pe cale amiabilă. În caz contrar, ele vor fi transmise spre examinare în instanța de judecată competentă conform cadrului normativ al Republicii Moldova.

12.2. Părțile contractante au dreptul, pe durata îndeplinirii contractului, să convină asupra modificării clauzelor contractului, prin acord adițional, numai în cazul apariției unor circumstanțe care lezează interesele comerciale legitime ale acestora și care nu au putut fi prevăzute la data încheierii contractului. Modificările și completările la prezentul Contract sunt valabile numai în cazul în care au fost perfectate în scris și au fost semnate de ambele Părți.

12.3. Nici una dintre Părți nu are dreptul să transmită obligațiile și drepturile sale stipulate în prezentul Contract unor terțe persoane fără acordul în scris al celeilalte părți.

12.4. Prezentul Contract în cazul în care este semnat electronic, de către ambele părți, acesta este remis în mod automat prin mijloacele electronice, dar în cazul când contractul este semnat olografic se întocmește în trei exemplare în limba română, câte un exemplar pentru Furnizor și două exemplare pentru Cumpărător.

12.5. Prezentul Contract se consideră încheiat la data semnării și intră în vigoare la data înregistrării la una din trezoreriile regionale ale Ministerului Finanțelor, în cazul în care sursele financiare se alocă din bugetul de stat/bugetul local, sau la data semnării sau la o altă dată ulterioară indicată în acest contract în cazul în care gestionarea surselor financiare nu se efectuează prin intermediul sistemului trezorerial.

12.6. Prezentul Contract este valabil până la 31 decembrie 2025, cu excepția pct. 1.5. al prezentului contract ce va rămâne valabil până la expirarea termenului indicat.

12.7. Prezentul Contract reprezintă acordul de voință al părților și se consideră semnat la data aplicării ultimei semnături de către una din părți.

12.8. Pentru confirmarea celor menționate mai sus, Părțile au semnat prezentul Contract în conformitate cu cadrului normativ al Republicii Moldova.

II. CONDIȚIILE SPECIALE A CONTRACTULUI

1.1. Suma penalității calculate Furnizorului conform prezentului Contract se va reține de către Cumpărător din suma garanției de bună executare a contractului.

1.2. Furnizorul va suporta toate costurile și formalitățile de import/export pentru livrarea bunurilor precum și riscurile care intervin, ducând marfa la destinație, precum și va asigura livrarea bunurilor până la Cumpărător cu implicarea personalului propriu.

1.3. Bunurile se consideră livrate de către Furnizor și acceptate de către Cumpărător după semnarea de către reprezentanții împuterniciți ai părților contractante a Actului de acceptanță finală a bunurilor livrate.

1.4. Persoanele responsabile de monitorizare a contractului din partea Cumpărătorului, la recepționarea bunurilor, în cazul unor nereguli depistate, va consemna în Actul de acceptanță finală, mențiunea despre tergiversare în vederea înaintării reclamațiilor motivate în acest sens.

1.5. Înlăturarea defecțiunilor depistate, în perioada de garanție va fi efectuată din contul Furnizorului, în cel mult 30 de zile din data sesizării.

DATELE JURIDICE, POȘTALE ȘI DE PLĂȚI ALE PĂRȚILOR

FURNIZOR	*CUMPĂRĂTOR*
SC „RAPID LINK" SRL	**Serviciul Tehnologii Informaționale al MAI**
mun. Chișinău, str Gh.Asachi,71/7 tel. 069222230, email: office@rapidlink.md	mun. Chișinău, str. Vasile Alecsandri, 42 tel. 022 255 269, email:sti@mai.gov.md
Cod fiscal : 1007600035161	Cod fiscal: 1013601000521
Banca: BC „OTP Bank" SA	Ministerul Finanțelor - Trezoreria de Chișinău, buget de stat
C/b: MOBBMD22	Cod bancar: TREZMD2X
IBAN: MD78MO2224ASV23214197100	**IBAN: MD80TRPBAA317110A00746AC**
SEMNĂTURILE PĂRȚILOR	
Administrator **Victor BACIU** Digitally signed by Baciu Victor Date: 2025.08.21 11:08:57 EEST Reason: MoldSign Signature Location: Moldova MOLDOVA EUROPEANĂ	**Director** **Ion BOTNARI** Digitally signed by Botnari Ion Date: 2025.08.21 13:49:49 EEST Reason: MoldSign Signature Location: Moldova MOLDOVA EUROPEANĂ
Președintele CI	Digitally signed by Capcelea Dorin Date: 2025.08.21 10:25:34 EEST Reason: MoldSign Signature Location: Moldova MOLDOVA EUROPEANĂ
SJ :	Digitally signed by Lisnic Ion Date: 2025.08.21 08:49:09 EEST Reason: MoldSign Signature Location: Moldova MOLDOVA EUROPEANĂ
SF :	Digitally signed by Curaciov Larisa Date: 2025.08.21 10:14:41 EEST Reason: MoldSign Signature Location: Moldova MOLDOVA EUROPEANĂ
Raportor DMISS	Digitally signed by Russu Dumitru Date: 2025.08.21 08:27:27 EEST Reason: MoldSign Signature Location: Moldova MOLDOVA EUROPEANĂ

Anexa nr. 1
la Contractul nr. 69
din 21.08.2025

SPECIFICAŢII TEHNICE

Denumirea bunurilor	Denumirea modelului bunurilor	Ţara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
Lotul 1 Implementarea Platformei Integrate de Monitorizare						
Platforma Integrată de Monitorizare	GENETEC Security Center	Canada	Genetec Inc	Conform Specificatiei tehnice și cerințe caietului de sarcini (Anexa nr. 3)	Conform Anexei nr.3, parte componentă a contractului și cerințelor obligatorii/opționale Platformei Integrate de Monitorizare	UL2900-2-3:2023 IS 670041 CLOUD 775314
SEMNĂTURILE PĂRŢILOR						
Administrator Victor BACIU _____ LŞ				**Director Ion BOTNARI** _____ LŞ		

Anexa nr. 2
la Contractul nr. 69
din 21.08.2025

SPECIFICAȚIA DE PREȚ

Cod CPV	Denumirea bunurilor	UM	Cantitatea	Preț unitar (fără TVA)	Preț unitar (cu TVA)	Suma fără TVA	Suma cu TVA	Termenul de livrare	Clasificație bugetară (IBAN)
1	2	3	4	5	6	7	8	9	10
Lotul 1 Implementarea Platformei Integrate de Monitorizare									
48200000-0	Platforma Integrată de Monitorizare (GENETEC Security Center / Irisity Iris + / VaxALPR)	Buc	1	6 050 000,00	7 260 000,00	6 050 000,00	7 260 000,00	*Termenul de livrare: până la 60 zile de la inregistrarea la MF*	MD80TRPBAA 317110A00746AC
	TOTAL					**6 050 000,00**	**7 260 000,00**		

SEMNĂTURILE PĂRȚILOR

Administrator Victor BACIU _____ LȘ	**Director Ion BOTNARI** _____ LȘ

Anexa nr. 3
la Contractul nr. 69
din 21.08.2025

CAIET DE SARCINI
Bunuri

Obiectul_____ **implementarea Platformei Integrate de Monitorizare**_____
(denumirea, adresa)

Autoritatea contractantă_____ **Serviciul Tehnologii Informaționale al MAI**_____

CUPRINS:

1. INTRODUCERE

Siguranța circulației rutiere și securitatea publică reprezintă provocări majore pentru Republica Moldova, având în vedere creșterea semnificativă a numărului de vehicule, intensificarea traficului și evoluția riscurilor asociate acestora.

În prezent, organele de aplicare a legii se confruntă cu dificultăți semnificative în monitorizarea și gestionarea incidentelor rutiere, menținerea ordinii publice și investigarea rapidă a evenimentelor ce necesită intervenție operativă. Aceste probleme sunt amplificate de lipsa unei infrastructuri centralizate și integrate, care să permită supravegherea eficientă, analiza inteligentă a datelor și răspunsul coordonat între instituțiile responsabile.

În acest context, Platforma integrată de monitorizare (PIM) vine ca o soluție strategică, menită să îmbunătățească procesele de supraveghere, intervenție și investigație. Aceasta va integra Sistemul automatizat de supraveghere a circulației rutiere „Controlul traficului", împreună cu alte componente esențiale de securitate publică, oferind autorităților un instrument unificat de gestionare a evenimentelor critice.

Implementarea PIM va transforma fundamental modul în care se realizează monitorizarea traficului, prevenirea infracțiunilor și gestionarea incidentelor, prin utilizarea tehnologiilor avansate de analiză și procesare a datelor.

1.1. Starea actuală și principalele probleme.

În prezent, lipsa unui sistem unificat de securitate creează mai multe dificultăți pentru organele de aplicare a legii, și anume:

- **fragmentarea infrastructurii de supraveghere** – existența unor sisteme disparate care nu comunică eficient între ele, ceea ce îngreunează schimbul rapid de informații și coordonarea intervențiilor.
- **capacitate limitată de analiză a datelor** – monitorizarea video și colectarea de informații sunt realizate în mare parte independent, fără corelarea datelor pentru identificarea tiparelor de risc și a zonelor vulnerabile.
- **reacție întârziată la incidente** – lipsa unui sistem integrat de alertare și intervenție face ca reacția la accidente, infracțiuni sau alte situații de urgență să fie mai lentă decât ar fi optim.
- **dificultăți în colectarea și gestionarea probelor digitale** – multe date relevante pentru investigații sunt fragmentate între diferite instituții, ceea ce îngreunează utilizarea lor eficientă în cadrul procedurilor judiciare.

1.2. Impactul implementării PIM

Implementarea PIM va elimina deficiențe expuse și va aduce următoarele îmbunătățiri:

- **crearea unei infrastructuri integrate** care va permite centralizarea și corelarea datelor provenite din diverse sisteme de supraveghere (*camere video inteligente, senzori de trafic, baze de date ale autorităților).*
- **analiză avansată a incidentelor** prin utilizarea tehnologiilor de procesare a datelor în timp real, facilitând detectarea timpurie a comportamentelor suspecte și intervenția proactivă.
- **optimizarea resurselor** forțelor de ordine prin alocarea inteligentă a echipajelor pe baza predicțiilor și analizelor de risc, reducând timpii de reacție și crescând eficiența operațională.
- **îmbunătățirea investigațiilor** prin acces rapid și securizat la date esențiale, precum înregistrări video, istoricul incidentelor și analiza comportamentală a vehiculelor și persoanelor implicate.
- **automatizarea proceselor** prin integrarea sistemelor de recunoaștere automată a numerelor de înmatriculare (ANPR) și a tehnologiilor de detectare a abaterilor rutiere.
- **creșterea nivelului de conformitate** cu legislația rutieră și penală, prin asigurarea cu probe digitale, care pot fi utilizate eficient în procesele administrative și judiciare.

1.3. Beneficiile viitoare pentru instituțiile statului și societate

Prin implementarea PIM, Republica Moldova va beneficia de:

- **siguranță rutieră sporită**, datorită monitorizării inteligente și măsurilor prompte de prevenire a accidentelor.
- **un climat de ordine publică mai stabil**, prin detectarea rapidă și gestionarea eficientă a incidentelor de securitate.

o **reducerea criminalității și creșterea eficienței investigațiilor**, prin utilizarea unei infrastructuri digitale avansate care va sprijini activitatea organelor de aplicare a legii.

o **optimizarea traficului urban și interurban**, bazată pe analiza în timp real a fluxului de circulație și intervențiile strategice în punctele critice.

o **reducerea costurilor operaționale pentru autorități**, prin automatizarea proceselor și eficientizarea resurselor umane și logistice.

Operatorii economici care doresc să participe la licitația publică pentru implementarea PIM **trebuie** să aibă în vedere că proiectul **necesită**:

✓ **expertiză în dezvoltarea și integrarea** soluțiilor IT pentru securitate publică și monitorizare video.

✓ **capacitate de a furniza soluții scalabile și interoperabile** care să permită integrarea cu infrastructura existentă.

✓ **soluții avansate de analiză a datelor** pentru procesarea informațiilor colectate din multiple surse.

✓ **capacitate de a asigura securitatea cibernetică și protecția datelor colectate**, în conformitate cu reglementările naționale și internaționale.

✓ **suport tehnic și mentenanță pe termen lung**, pentru a asigura funcționarea optimă a sistemului și adaptarea acestuia la noile provocări din domeniul securității.

Implementarea PIM reprezintă un pas major în creșterea siguranței rutiere și a ordinii publice în Republica Moldova. Modernizarea sistemului „Controlul traficului" și integrarea acestuia cu infrastructura de securitate publică va aduce beneficii semnificative atât pentru autorități, cât și pentru cetățeni.

Prin utilizarea tehnologiilor avansate, acest proiect va permite o mai bună prevenire a incidentelor, o reacție rapidă a organelor de aplicare a legii și o eficiență sporită în investigarea infracțiunilor și contravențiilor.

Pentru operatorii economici interesați de participarea la licitație, proiectul oferă oportunitatea de a contribui la dezvoltarea unui sistem modern și eficient de securitate națională, consolidând astfel poziția Republicii Moldova ca stat care adoptă soluții inteligente pentru gestionarea siguranței publice și a traficului rutier.

2. OBIECTIVELE PROIECTULUI

Proiectul va facilita monitorizarea avansată a traficului și a comportamentului urban, utilizând tehnologii inteligente pentru a sprijini deciziile autorităților în timp real. Operatorii economici interesați de participarea la licitație trebuie să asigure soluții scalabile, interoperabile și conforme cu standardele internaționale de securitate.

Implementarea PIM urmărește crearea unui sistem modern, integrat și eficient, care să îmbunătățească siguranța rutieră, ordinea publică și capacitatea de investigare a incidentelor, și anume:

2.1. îmbunătățirea siguranței publice.

Un obiectiv strategic al acestui proiect este reducerea riscurilor pentru siguranța cetățenilor printr-un sistem inteligent de supraveghere și intervenție. Integrarea camerele ANPR (Automatic Number Plate Recognition) și PTZ (Pan-Tilt-Zoom) va permite:

–monitorizarea continuă a traficului și comportamentului rutier, identificând în timp real abaterile de la legislație și sancționând automat încălcările normelor de circulație;

–creșterea eficienței intervenției autorităților, prin detectarea rapidă a vehiculelor suspecte sau a activităților ilicite, facilitând intervențiile structurilor de ordine publică;

–prevenirea și reducerea accidentelor prin analiza tiparelor de comportament în trafic și luarea de măsuri proactive pentru zonele cu risc ridicat;

–sprijinirea investigațiilor prin acces rapid la datele colectate, inclusiv traseul vehiculelor implicate în infracțiuni sau incidente rutiere.

Operatorii economici trebuie să ofere soluții tehnologice avansate pentru colectarea, procesarea și interpretarea datelor în timp real, facilitând astfel intervențiile rapide și eficiente ale autorităților.

2.2. suport pentru decizii informatizate.

PIM va integra un sistem avansat de analiză a datelor care va sprijini factorii de decizie în planificarea și gestionarea traficului, siguranței publice și investigațiilor. Implementarea unei platforme de colectare și corelare a datelor va permite:

–generarea automată a rapoartelor și analizelor predictive, evidențiind zonele cu risc ridicat și tiparele de încălcări ale normelor de siguranță;

–monitorizarea și investigarea eficientă a incidentelor, folosind camere PTZ cu funcționalități avansate de urmărire și analiză video;

–optimizarea resurselor autorităților, prin alocarea echipajelor în funcție de analiza în timp real a fluxului de trafic și a evenimentelor de securitate;

–detectarea timpurie a amenințărilor și comportamentelor suspecte, folosind inteligența artificială pentru analizarea volumului mare de date colectate.

Operatorii economici trebuie să propună soluții care includ procesare AI/Big Data și algoritmi de învățare automată, pentru crearea unei infrastructuri sigure și eficiente de analiză a datelor.

2.3. alinierea la standardele internaționale.

Pentru a asigura securitatea și conformitatea sistemului, proiectul va fi dezvoltat în conformitate cu standarde internaționale de protecție a datelor și securitate cibernetică. Aceasta include:

–certificări ISO/IEC 27001 pentru securitatea informațiilor, garantând protecția datelor colectate și respectarea cerințelor GDPR și NIS 2.

–implementarea protocoalelor de criptare și protecție a infrastructurii IT, pentru a preveni atacurile cibernetice asupra sistemului;

–interoperabilitate cu alte sisteme naționale și internaționale de securitate, asigurând un schimb eficient de informații cu structurile de aplicare a legii;

–respectarea cerințelor UE privind protecția infrastructurilor critice, oferind autorităților un mediu de lucru sigur și fiabil.

Operatorii economici trebuie să furnizeze soluții certificate și conforme cu cerințele internaționale, asigurând securitatea, protecția datelor și funcționarea optimă a sistemului pe termen lung.

2.4. Interconectare și colaborare eficientă între entitățile responsabile.

Un aspect esențial al PIM este crearea unui ecosistem în care instituțiile responsabile să colaboreze eficient. Acest obiectiv presupune:

–integrarea sistemelor existente la nivelul Ministerului Afacerilor Interne, Agenției Servicii Publice, serviciilor de urgență și altor entități relevante pentru schimbul rapid de informații.

–automatizarea proceselor de alertare și coordonare a echipajelor, reducând timpul de reacție în caz de incidente critice.

–crearea unei arhitecturi deschise și scalabile, care să permită adăugarea de noi module și tehnologii pe măsură ce evoluează nevoile de securitate.

Operatorii economici trebuie să propună soluții software și hardware compatibile cu arhitectura modulară, care să permită dezvoltarea și extinderea ulterioară a platformei.

Obiectivele PIM sunt orientate spre îmbunătățirea siguranței publice, optimizarea deciziilor bazate pe date, alinierea la standardele internaționale și facilitarea colaborării între instituțiile responsabile.

Operatorii economici care doresc să participe la licitație trebuie să demonstreze capacitatea de a furniza soluții tehnologice avansate, interoperabile și conforme cu cerințele internaționale, contribuind astfel la crearea unui sistem eficient și modern de securitate publică.

3. OBIECTUL ACHIZIȚIEI

Obiectul achiziției îl reprezintă procurarea unei Platforme Integrate de Monitorizare (PIM), o soluție software avansată, capabilă să gestioneze, coreleze și controleze multiple subsisteme și module de securitate publică și siguranță rutieră. Aceasta trebuie să ofere o **interfață unificată** pentru vizualizare și administrare, centralizând datele operaționale, optimizând gestionarea evenimentelor și facilitând procesele decizionale ale autorităților competente. Totodată, platforma trebuie să fie **interoperabilă** și **flexibilă**, permițând integrarea eficientă cu infrastructuri existente și sistemele utilizate de instituțiile responsabile de securitate și ordine publică.

3.1. Caracteristici generale

3.1.1. Interfață unică și integrată – un punct central de acces și control, care reunește toate fluxurile de date provenite din diverse subsisteme, precum:

a. supraveghere video clasică și inteligentă;

b. recunoaștere automată a numerelor de înmatriculare (ANPR);

c. control acces și securitate perimetrală;

d. analiză comportamentală și detectare anomalii.

Aceasta trebuie să permită operatorilor o experiență intuitivă, facilitând monitorizarea în timp real, gestionarea alertelor și raportarea incidentelor, fără a fi necesară comutarea între platforme disparate.

3.1.2. Scalabilitate și interoperabilitate – trebuie să fie de tip Enterprise, utilizată și testată în scenarii operaționale complexe, cu capacitate demonstrată de scalabilitate și integrare. PIM trebuie să permită:

a. extinderea modulară prin adăugarea de noi funcționalități și echipamente;

b. interoperabilitate cu infrastructuri existente pentru protejarea investițiilor anterioare;

c. automatizarea proceselor operaționale prin generarea de alerte inteligente în timp real și furnizarea de analize avansate.

3.1.3. Funcționalități avansate – trebuie să ofere suport pentru tehnologii avansate, inclusiv:

a. analiză video inteligentă pentru detectarea comportamentelor anormale în trafic și spațiul public;

b. gestionarea incidentelor prin colectarea și corelarea datelor din multiple surse;

c. automatizarea monitorizării încălcărilor regulilor de circulație;

d. raportare avansată și vizualizare analitică pentru optimizarea intervențiilor autorităților.

3.1.4. Compatibilitate și integrare – trebuie să permită integrarea fără întreruperi cu echipamentele existente și să asigure:

a. compatibilitate cu camerele ANPR deja instalate și cu viitoarele extinderi ale rețelei de supraveghere;

b. suport pentru standarde deschise și interfețe API, permițând integrarea cu alte sisteme de management urban;

c. flexibilitate în adaptarea la infrastructura IT existentă, fără a impune limitări tehnologice.

Soluția achiziționată va deveni un instrument esențial pentru autoritățile competente, facilitând monitorizarea continuă, gestionarea evenimentelor și luarea deciziilor bazate pe intelligence.

Platforma trebuie să fie scalabilă, interoperabilă și robustă, contribuind la creșterea eficienței operaționale, îmbunătățirea siguranței publice și protejarea infrastructurii critice.

3.2. Lista de livrabile și servicii.

Nr.	Denumire	Descriere succintă
1.	**Platforma Integrată de Monitorizare**	Platforma integrată de Monitorizare va asigura monitorizarea, analiza fluxurilor video și gestionarea datelor colectate de camerele ANPR și alte sisteme de captare și supraveghere. Aceasta va include toate licențele necesare pentru operare și funcționalitate optimă, garantând compatibilitate cu un număr minim de 500 fluxuri video pentru monitorizare, având capacități extinse de analiză și management, astfel: • Minim 125 dispozitive ANPR cu procesare server-based (4K); • Minim 100 dispozitive pentru analiză video avansată (server-based); • Minim 20 dispozitive pentru recunoaștere facială (server-based); • Minim 20 utilizatori concomitenți pentru platforma integrată; • Minim 15 utilizatori concomitenți pentru componenta de analiză video avansată; • Minim 15 utilizatori concomitenți pentru componenta de gestionare a incidentelor; • Minim 10 conexiuni concurente pentru componenta API.
2.	**Suport tehnic și garanție**	Instalare și configurare: Implementarea platformei, adaptată la fluxurile operaționale ale beneficiarului, asigurând integrarea eficientă în infrastructura existentă. Garanție și suport tehnic: Asigurarea unei perioade minime de 3 ani de suport tehnic pentru toate echipamentele și soluțiile software furnizate, careva include obligatoriu:

		a. înlocuirea componentelor defecte; b. actualizările software necesare pentru menținerea funcționalității și securității platformei; c. soluționarea rapidă (max. 24h) a eventualelor probleme tehnice. Instruire utilizatori și administratori: Organizarea sesiunilor dedicate pentru: a. administrarea platformei; b. utilizarea în diferite scenarii de către beneficiari finali; c. configurarea alertelor și gestionarea incidentelor; d. optimizarea utilizării datelor colectate pentru analiză și raportare; e. elaborarea rapoartelor. Suport tehnic specializat („Professional Services") pentru o perioadă de cel puțin 3 ani, incluzând: a. asistență continuă în exploatarea și utilizarea platformei; b. intervenții tehnice rapide, atât de la distanță, cât și la fața locului, pentru menținerea funcționalității și continuitatea operațiunilor.

3.3. Termene și Cerințe de Conformitate

3.3.1. Platforma trebuie livrată în termen de maximum **60 de zile** de la data semnării și înregistrării contractului.

3.3.2. După livrare, platforma va fi supusă unui test de acceptanță de 30 de zile, în condiții reale, pentru a verifica conformitatea cu cerințele funcționale și de performanță, după care Beneficiarul va furniza actul de acceptanță finală.

3.3.3. Cerințe minime și demonstrarea conformității. Toate cerințele din prezentul document sunt **prescriptive** și minimale, iar ofertantul trebuie să demonstreze conformitatea acestora prin informații clare și dovezi verificabile. Conformitatea trebuie să fie susținută prin:

a. certificări relevante;
b. rapoarte oficiale de testare;
c. scrisori de recomandare de la clienți;
d. alte documente justificative care atestă îndeplinirea specificațiilor tehnice și operaționale.

Oferta tehnică trebuie să includă o matrice de conformitate, în care să fie specificat clar modul în care platforma ofertată îndeplinește fiecare cerință. Pentru fiecare punct de conformitate, ofertantul trebuie să furnizeze dovezi clare, inclusiv referințe la documentația tehnică oficială și alte materiale justificative relevante. În absența acestei matrice sau în cazul în care conformitatea nu este demonstrată corespunzător, oferta va fi considerată neconformă.

Respectarea ofertei inițiale. În cadrul procesului de clarificare și evaluare a ofertelor, dacă ofertantul furnizează informații, soluții sau specificații tehnice care nu au fost incluse în oferta inițială, acestea vor fi considerate modificări ale ofertei inițiale. În acest caz, oferta va fi respinsă și declarată neconformă.

Validarea funcționalităților și tehnologiilor utilizate: Ofertantul trebuie să asigure că toate funcționalitățile și parametrii de operare specificați sunt validați în condiții reale de utilizare, iar tehnologiile propuse sunt mature, testate și implementate în proiecte similare în spațiul UE.

Echivalențe și deviații. Orice deviație de la cerințele impuse trebuie să fie documentată și justificată clar, iar orice soluție echivalentă propusă trebuie să fie demonstrabilă prin documentație oficială și referințe verificabile.

4. CERINȚE GENERALE FAȚĂ DE PIM

4.1. Cerințe generale.

Această secțiune definește **principiile fundamentale** pe care trebuie să le îndeplinească platforma destinată modernizării și extinderii sistemului de supraveghere a traficului rutier și a siguranței publice. Soluția trebuie să asigure un cadru tehnologic unificat, capabil să gestioneze centralizat fluxurile video, datele operaționale și incidentele, oferind în același timp:

a. compatibilitate extinsă cu echipamentele existente;
b. interoperabilitate cu sisteme terțe utilizate de autorități;

c. un nivel ridicat de securitate cibernetică, asigurând protecția infrastructurii critice.

PIM trebuie să permită agregarea, analiza și corelarea datelor provenite din multiple surse, inclusiv:

a. camere ANPR pentru identificarea și gestionarea traficului rutier;

b. camere PTZ pentru supravegherea zonelor critice și urmărirea inteligentă a incidentelor;

c. senzori și dispozitive de monitorizare pentru detectarea evenimentelor în timp real;

d. sisteme informaționale și baze de date operaționale pentru corelarea informațiilor și optimizarea procesului decizional.

Soluția trebuie să furnizeze instrumente avansate de monitorizare, investigare și luare a deciziilor, utilizând tehnologii moderne, precum:

a. inteligență artificială pentru detectarea și prevenirea incidentelor;

b. analiză video predictivă, care să sprijine intervențiile proactive și managementul eficient al resurselor.

4.2. Cerințe specifice.

PIM reprezintă **elementul central al soluției**, fiind responsabilă de gestionarea integrată a tuturor componentelor sistemului. Aceasta trebuie să fie concepută astfel încât să permită centralizarea și automatizarea proceselor operaționale, facilitând coordonarea eficientă și reacția rapidă la evenimente critice.

Pentru a răspunde cerințelor actuale și viitoare, platforma trebuie să fie:

a. scalabilă și modulară, permițând extinderea fără constrângeri tehnologice sau arhitecturale;

b. interoperabilă, capabilă să se integreze cu sisteme terțe și echipamente multi-vendor, utilizând standarde deschise și API-uri moderne;

c. automatizată și inteligentă, oferind funcționalități avansate de analiză video, detecție automată a incidentelor și corelare în timp real;

d. sigură, implementând protocoale avansate de criptare, autentificare multi-factor (MFA) și mecanisme robuste de protecție împotriva atacurilor cibernetice;

e. fiabilă și rezilientă, prin suportul pentru redundanță, recuperare automată în caz de defecțiune și operare continuă 24/7.

4.2.1. Interfață unificată de management și control.

Interfața unificată de management și control reprezintă **punctul central de dirijare** al platformei, reunind toate componentele și subsistemele într-un tablou de bord integrat și ușor accesibil utilizatorilor autorizați. Aceasta trebuie să ofere o experiență intuitivă și eficientă, permițând gestionarea în timp real a fluxurilor video, incidentelor și alertelor, fără a necesita comutarea între sisteme disparate.

Caracteristici esențiale ale interfeței unificate:

a. acces centralizat la toate modulele funcționale ale platformei (*supraveghere video, ANPR, analiză comportamentală, control acces, gestionare incidente etc.);*

b. vizualizare integrată și dinamică a tuturor fluxurilor video și evenimentelor relevante, cu posibilitatea de filtrare și personalizare a afișării;

c. capacitate avansată de control asupra dispozitivelor (ex. camere PTZ – panoramare, zoom, ajustarea unghiului de vizualizare);

d. notificări și alerte contextuale, cu posibilitatea configurării scenariilor automate de reacție la evenimente;

e. audit și jurnalizare avansată, pentru monitorizarea și verificarea acțiunilor utilizatorilor.

Interfață trebuie să fie adaptabilă nevoilor operatorilor, oferind personalizare în funcție de roluri, astfel încât fiecare utilizator să aibă acces doar la informațiile și funcționalitățile relevante pentru activitatea sa. De asemenea, trebuie să fie compatibilă cu dispozitive mobile, permițând operarea și monitorizarea de la distanță, în condiții de securitate maximă, conform cerințelor expuse în tabelul de mai jos:

Nr.	Cerință
1.	Platforma Integrată de Monitorizare (în continuare – platforma) trebuie să fie o soluție software integrată, care să combine și să gestioneze centralizat toate subsistemele și modulele de securitate relevante. Platforma trebuie să asigure centralizarea și corelarea tuturor datelor generate de dispozitivele conectate, permițând vizualizarea, administrarea și analiza acestora într-un mediu unic de operare.

2.	Platforma și toate componentele/subsistemele și modulele acesteia trebuie să fie o soluție matură și testată în timp, utilizată în implementări operaționale demonstrabile la nivel internațional. Aceasta trebuie să fie validată prin utilizare în multiple scenarii reale, având referințe documentate în cel puțin trei țări și operând în medii cu cerințe ridicate de fiabilitate, securitate și performanță. Pentru a fi considerată Enterprise/Industrial Grade, platforma trebuie să îndeplinească următoarele criterii: a. fiabilitate și disponibilitate ridicată: suport pentru operare continuă 24/7/365, cu un timp de disponibilitate garantat de minimum 99.9%. b. scalabilitate dovedită: capacitatea de a gestiona simultan un număr ridicat de dispozitive (min 5000), fluxuri video și utilizatori, fără degradarea performanței. c. specializare: proiectată și dezvoltată în scopuri de securitate, monitorizare și analiză. d. testare și validare în medii operaționale: trebuie să fie deja implementată și să funcționeze de minimum 5 ani în scenarii similare, demonstrând stabilitate și eficiență. e. interoperabilitate extinsă: compatibilitate nativă cu standarde internaționale deschise (de ex. ONVIF, RTSP, REST API), care să permită integrarea cu alte sisteme și infrastructuri existente. f. certificări și conformitate: trebuie să implementeze cerințele de securitate conform standardelor internaționale relevante pentru securitate, protecția datelor și continuitatea operațională. g. reputație și referințe documentate: utilizată în scop similar al obiectului achiziției în cel puțin două state, cu referințe disponibile la cerere. **h. informația despre platforma este disponibilă public și nu are restricții la achiziționare/comercializare.**
3.	Platforma trebuie să fie scalabilă și modulară, permițând extinderea fără întreruperi operaționale prin adăugarea de noi dispozitive, module funcționale și utilizatori. Scalabilitatea trebuie să fie asigurată atât la nivel tehnologic (*suport pentru volume crescute de date și fluxuri video*), cât și la nivel funcțional (*posibilitatea de integrare cu noi sisteme și echipamente, fără limitări arhitecturale impuse de soluție*).
4.	Platforma trebuie să ofere o interfață unificată de gestionare și control, care să permită administrarea centralizată a cel puțin următoarelor module funcționale/subsisteme: a. modul de gestionare a evenimentelor de trafic rutier, bazat pe recunoașterea numerelor de înmatriculare (ANPR); b. modul de gestionare video (VMS), responsabil pentru înregistrarea, arhivarea și vizualizarea fluxurilor video; c. modul de gestionare a situațiilor de interes, destinat organizării și corelării evenimentelor relevante pentru siguranța rutieră și publică; d. modul de analiză inteligentă a fluxurilor video, capabil să detecteze automat comportamente anormale, obiecte abandonate, congestii sau alte scenarii de interes.
5.	Platforma va include nativ toate modulele funcționale/subsisteme enumerate la cerința 4, fără a necesita integrarea prin soluții externe, plugin-uri suplimentare sau dezvoltări personalizate. Fiecare modul trebuie să fie dezvoltat și menținut de același producător, asigurând compatibilitate deplină, actualizări uniforme și suport tehnic unificat.
6.	Platforma trebuie să asigure interfața unificată de gestionare și control pentru administrarea centralizată suplimentară a cel puțin următoarelor module funcționale/subsisteme, incluse: a.Modul de gestionare a dispozitivelor IoT, destinat monitorizării și controlului senzorilor și altor dispozitive conectate la infrastructura de securitate; b.Modul de control al accesului, care reglementează și monitorizează accesul în zone securizate pe baza autentificării electronice; c.Modul de control perimetral, care gestionează detecția și răspunsul la incidente la nivelul punctelor de control și al sistemelor de securitate perimetrală.
7.	Platforma trebuie să permită monitorizarea în timp real a tuturor fluxurilor video și datelor capturate, oferind acces instantaneu, securizat și neîntrerupt la toate informațiile esențiale prin intermediul unui tablou de bord unic și unificat. Platforma trebuie să suporte: a. Vizualizare simultană a cel puțin 50 fluxuri video per operator;

	b. Acces rapid la istoricul evenimentelor și arhiva video, cu posibilitatea de căutare avansată pe baza metadatelor; c. Notificări și alerte contextuale pentru incidente, afișate direct în interfața de operare.
8.	Platforma trebuie să permită personalizarea tablourilor de bord pentru fiecare utilizator/operator, asigurând configurarea vizualizării datelor conform preferințelor și nevoilor specifice. Personalizarea trebuie să includă: a. selecția și aranjarea widget-urilor în funcție de rolul și responsabilitățile fiecărui utilizator; b. filtrarea și afișarea informațiilor relevante pe baza drepturilor de acces și nivelului de autorizare; c. setarea alertelor și notificărilor specifice pentru evenimente și situații de interes.
9.	Platforma trebuie să asigure accesibilitatea tuturor componentelor și modulelor funcționale integrate prin intermediul unei interfețe unificate, oferind operatorilor o vizualizare coerentă și eficientă a datelor și evenimentelor în timp real.
10.	Platforma trebuie să includă un sistem unificat de notificări cu posibilitatea de personalizare, care să alerteze operatorii în caz de incidente critice sau situații de interes, aplicabile pentru toate module și subsistemele.
11.	Platforma trebuie să permită controlul și dirijarea dispozitivelor de monitorizare video direct din interfața de management, permițând operatorilor să ajusteze unghiul de vizualizare, zoom-ul și focalizarea camerelor în timp real.
12.	Platforma trebuie să ofere suport pentru mai multe limbi, inclusiv Română și Engleză, asigurând astfel accesibilitate pentru toți utilizatorii.
13.	Platforma trebuie să asigure audit și jurnalizare centralizată și unificată pentru toate modulele și subsistemele, permițând monitorizarea și verificarea accesului și acțiunilor utilizatorilor în sistem. Funcționalitatea de audit trebuie să înregistreze toate evenimentele relevante, inclusiv autentificarea, modificările de configurare, accesul la date și operațiunile critice, asigurând trasabilitate completă și conformitate cu cerințele de securitate.
14.	Platforma trebuie să asigure gestionarea centralizată și unificată a alarmelor și incidentelor pentru toate modulele și subsistemele, permițând monitorizarea, clasificarea și raportarea acestora în timp real. Sistemul de gestionare a evenimentelor/incidentelor trebuie să includă mecanisme automate de escaladare, declanșând un flux de lucru predefinit de beneficiar, care poate implica notificarea operatorilor desemnați, atribuirea sarcinilor și coordonarea intervențiilor conform procedurilor stabilite.
15.	Platforma trebuie să asigure configurarea centralizată și unificată a fluxurilor de lucru automatizate pentru toate modulele și subsistemele, permițând definirea, personalizarea și gestionarea dinamică a scenariilor operaționale. Platforma trebuie să permită crearea și modificarea fluxurilor complexe de automatizare prin interfață grafică de tip drag-and-drop, oferind operatorilor posibilitatea de a defini reguli, condiții și acțiuni fără a fi necesare intervenții tehnice avansate. Fluxurile de lucru automatizate trebuie să suporte: a. declanșarea automată a acțiunilor și notificărilor în baza evenimentelor detectate (ex: identificarea vehiculelor de interes, acces neautorizat, alarme de securitate); b. escaladarea dinamică a incidentelor conform scenariilor definite de beneficiar; c. integrarea cu module externe pentru coordonarea automată a intervențiilor și gestionarea resurselor operative; d. monitorizare și ajustare în timp real a fluxurilor, permițând optimizarea continuă a proceselor operaționale.
16.	Platforma trebuie să asigure gestionarea centralizată și unificată a drepturilor de acces și privilegiilor utilizatorilor pentru toate modulele și subsistemele, permițând actualizarea dinamică a permisiunilor. Sistemul de administrare a accesului trebuie să ofere posibilitatea de definire și personalizare a rolurilor specifice, în funcție de responsabilitățile fiecărui operator, asigurând aplicarea coerentă a politicilor de securitate și respectarea principiului accesului minim necesar (Least Privilege Access).
17.	Platforma trebuie să fie compatibilă cu dispozitive mobile, oferind acces securizat la funcționalitățile critice și din afara locațiilor fixe de lucru.

18.	Platforma trebuie să permită vizualizarea și gestionarea hărților interactive, oferind localizarea geografică a dispozitivelor, afișarea incidentelor și monitorizarea activităților în funcție de locație.

4.2.2. Cerințe față de interoperabilitate și integrare

Nr.	Cerință
19.	Platforma trebuie să aibă o arhitectură deschisă, care să permită integrarea ușoară cu echipamente și sisteme furnizate de terți (3rd party), inclusiv camere de supraveghere; sisteme de video management; sisteme de control al accesului; soluții de analiză video; sisteme anti-incendiu; alte sisteme/sub-sisteme de securitate și/sau management fluxuri operaționale.
20.	Platforma trebuie să permită integrarea cu sisteme de supraveghere video existente, inclusiv suport pentru camere IP de la diferiți producători, asigurând compatibilitatea cu echipamentele deja instalate.
21.	Platforma trebuie să integreze și să gestioneze cel puțin următoarele echipamente existente, asigurând compatibilitate și operare centralizată: a. Camere PTZ - DS-2DE4425IW-DET5 - 5 unități; b. Camere iDS-TCV907-BIR/C – min 25 dispozitive; c. Camere iDS-TCV900-HI – 100 unități; d. Camere PTZ - DS-2SE7C432MWG-EB/26(F0) - 15 unități; e. Camere PTZ - DS-2DE7232IW-AE - 13 unități.
22.	Platforma trebuie să asigure compatibilitate nativă și interoperabilitate completă cu camerele ANPR produse de producători renumiți din industrie, permițând integrarea fără probleme și utilizarea tuturor funcționalităților avansate disponibile. Compatibilitatea trebuie să includă, dar nu se limitează la, următorii producători: a.Axis Communications b.Bosch Security Systems c.Hanwha Techwin d.Motorola Solutions e.Sony f. Panasonic g.Vivotek h.Pelco Integrarea cu camerele ANPR nu trebuie să se limiteze la fluxurile video, ci trebuie să permită extragerea, procesarea și corelarea tuturor metadatelor disponibile direct din dispozitiv, inclusiv: a.numărul de înmatriculare al vehiculului recunoscut; b.viteza vehiculului, dacă este furnizată de cameră; c.locația și ora exactă a capturii, bazate pe coordonatele GPS sau metadatele camerei; d.tipul, modelul și culoarea vehiculului, dacă sunt detectate de algoritmul camerei; e.indicele de încredere al recunoașterii, pentru validarea și filtrarea datelor; f. pozele relevante aferente evenimentului (traversare sau incalcare); g.informația aferenta încălcărilor (RedLight, CrossLine, etc), daca sunt detectate de algoritmul camerei. h.alte metadate relevante.
23.	Platforma trebuie să permită integrarea cu sisteme de video management terțe (VMS), control acces și alte soluții de securitate, utilizând protocoale standardizate precum ONVIF, PSIA, RTSP, SIP, HTTPS, TLS, și API-uri REST pentru a asigura interoperabilitatea și schimbul de date fără întreruperi.
24.	Platforma trebuie să ofere suport pentru integrarea soluțiilor de recunoaștere facială, ANPR și alte tehnologii avansate de identificare, altele decât cele solicitate, permițând extinderea capabilităților de monitorizare și analiză a traficului și securității publice.
25.	Platforma trebuie să asigure compatibilitatea cu soluțiile de analiză video și management al incidentelor, permițând corelarea datelor din multiple surse și facilitând generarea automată de rapoarte și analize pentru decizii operaționale rapide.

26.	Platforma trebuie să includă nativ integrări cu sisteme de gestionare a traficului şi infrastructurii rutiere, permiţând controlul şi monitorizarea în timp real a fluxurilor de vehicule, semafoarelor, barierelor automate şi altor dispozitive de gestionare a traficului. Integrarea trebuie să fie nativă şi complet funcţională în platformă, fără a necesita dezvoltări suplimentare, achiziţia de module adiţionale sau personalizări care ar putea genera costuri neprevăzute. Platforma trebuie să asigure compatibilitate directă cu protocoalele şi standardele utilizate în industria gestionării traficului, permiţând: a. controlul şi automatizarea semafoarelor, bazat pe fluxul de trafic detectat şi scenarii predefinite; b. gestionarea barierelor automate şi a sistemelor de acces controlat, prin corelarea cu evenimentele detectate de camerele ANPR şi alte senzori; c. monitorizarea şi analiza în timp real a traficului, prin integrarea cu senzori rutieri, radare şi alte dispozitive de măsurare; d. generarea de alerte şi acţiuni automate, pe baza anomaliilor detectate sau a condiţiilor predefinite de trafic. Platforma trebuie să ofere interfaţă nativă de administrare şi configurare a dispozitivelor, fără a necesita dezvoltări ulterioare, garantând astfel un proces de integrare eficient, predictibil şi fără riscuri financiare suplimentare.
27.	Platforma trebuie să permită integrarea cu soluţii de stocare şi arhivare terţe, permiţând stocarea în siguranţă a datelor video şi ANPR pe termen lung, cu suport pentru sisteme locale şi de tip cloud.
28.	Platforma trebuie să includă nativ integrarea cu sisteme IoT (Internet of Things) permiţând monitorizarea, controlul şi analiza în timp real a dispozitivelor conectate din infrastructura de securitate şi trafic. Aceasta trebuie să ofere un cadru unificat de administrare, care să asigure interoperabilitatea cu o gamă variată de senzori şi dispozitive IoT, fără necesitatea unor dezvoltări suplimentare sau personalizări costisitoare. Aceasta trebuie să includă cel puţin, dar fără a se limita la: a. gestionarea centralizată a dispozitivelor IoT, inclusiv senzori de mediu, detectoare de mişcare, contoare inteligente, radare şi alte dispozitive din infrastructura rutieră şi de securitate; b. vizualizare unificată a datelor IoT în tabloul de bord al platformei, cu posibilitatea de corelare între evenimente, fluxuri video şi datele furnizate de senzori; c. monitorizarea şi analiza în timp real a parametrilor critici, cum ar fi nivelul de trafic, condiţiile meteorologice, iluminatul stradal sau consumul de energie al dispozitivelor conectate; d. automatizarea scenariilor operaţionale, prin definirea de fluxuri de lucru bazate pe date IoT (*de exemplu, activarea automată a iluminatului public sau ajustarea timpilor semafoarelor în funcţie de fluxul de trafic detectat*); e. suport pentru protocoale de comunicaţie standardizate utilizate în domeniul IoT, cum ar fi MQTT, HTTPS, REST API şi WebSockets, asigurând interoperabilitate extinsă cu dispozitive multi-vendor; f. mecanisme avansate de securitate pentru dispozitivele IoT, incluzând autentificare bazată pe certificate digitale, criptare end-to-end şi politici de acces granular pentru protecţia datelor şi prevenirea atacurilor cibernetice; g. capacitate de extindere dinamică, permiţând adăugarea şi administrarea de noi dispozitive IoT fără a necesita dezvoltări suplimentare.
29.	Platforma trebuie să suporte integrarea cu protocoale standard de comunicare, cum ar fi Modbus, BACnet, MQTT, OPC şi SNMP, pentru a asigura conectivitatea şi interoperabilitatea între diverse sisteme.
30.	Platforma trebuie să includă nativ suport pentru integrarea cu soluţii de comunicaţii securizate, inclusiv VoIP, pentru a asigura coordonarea rapidă şi eficientă a echipelor de intervenţie şi schimbul de informaţii în timp real între operatori şi autorităţi. Aceasta trebuie sa includă cel puţin, dar fără a se limita la : a. integrare cu infrastructura VoIP existentă, utilizând standarde deschise precum SIP (Session Initiation Protocol), fără a necesita module suplimentare sau dezvoltări personalizate; b. capacitate de iniţiere şi gestionare a apelurilor VoIP direct din interfaţa platformei, permiţând operatorilor să comunice rapid cu echipele din teren sau alte centre de comandă;

	c. integrarea apelurilor VoIP cu fluxurile video și datele din platformă, oferind operatorilor posibilitatea de a vizualiza și corela apelurile cu evenimentele monitorizate (de exemplu, apelarea directă a unui echipaj atunci când este detectat un incident); d. funcționalități avansate de rutare și escaladare automată a apelurilor, pe baza fluxurilor de lucru definite de beneficiar (ex. direcționarea apelurilor către operatori disponibili, redirecționare automată către autorități etc.); e. securizarea comunicațiilor prin criptare end-to-end și autentificare multi-factor, prevenind interceptarea și accesul neautorizat la datele transmise.
31.	Platforma trebuie să suporte adăugarea și gestionarea de conectori pentru integrarea soluțiilor terțe, permițând extinderea capacităților sistemului fără modificări majore în infrastructură, asigurând astfel flexibilitate și scalabilitate.
32.	Platforma trebuie să includă nativ suport pentru integrarea cu soluții terțe de reprezentare geografică (GIS MAP), asigurând vizualizarea și corelarea evenimentelor și dispozitivelor într-un context geospațial. Aceasta trebuie să fie compatibilă cel puțin cu următoarele platforme de cartografiere: a.ArcGIS b. Google Maps c. Bing Maps d. OpenStreetMap Aceasta trebuie sa includă cel puțin, dar fără a se limita la : a.afișarea în timp real a dispozitivelor și evenimentelor pe hartă, inclusiv poziționarea camerelor, senzorilor, vehiculelor monitorizate și incidentelor detectate; b. integrarea cu sisteme de camere ALPR (Automatic License Plate Recognition) fixe și mobile pentru localizarea precisă a vehiculelor de interes. c. suport pentru suprapunerea de layere personalizabile, permițând afișarea infrastructurilor critice, zonelor de restricție; d. capacitate de integrare cu surse externe de date geospațiale, permițând încărcarea și actualizarea automată a hărților, bazelor de date GIS și informațiilor de trafic; e. interoperabilitate prin standarde deschise, utilizând protocoale precum WMS (Web Map Service), WFS (Web Feature Service) și REST API, pentru schimb de date cu alte sisteme GIS; f. clasificarea incidentelor în funcție de severitate, tip și zonă geografică. Utilizatorii pot crea și gestiona incidente, atribuindu-le niveluri de severitate și categorizându-le;
33.	Platforma trebuie să suporte importul și exportul de date între sisteme terțe, asigurând interoperabilitatea și sincronizarea continuă a datelor critice pentru monitorizare și analiză.
34.	Platforma trebuie să suporte integrarea cu soluții de automatizare și machine learning pentru analiza predictivă, permițând dezvoltarea de soluții personalizate și extinderea funcționalităților în funcție de nevoile organizației.
35.	Platforma trebuie să permită implementarea și gestionarea mecanismelor de autentificare puternică, compatibile cu standardele OpenID Connect și SAML 2.0, asigurând că toate comunicările între utilizatori și sistem sunt autentificate și protejate corespunzător.
36.	Platforma trebuie să sprijine utilizarea discurilor NAS, PC-uri și alte echipamente de stocare din rețele LAN/WAN, oferind suport pentru arhivarea flexibilă a fluxurilor video și datelor colectate într-un mediu distribuit, fără dependențe de soluții proprietare.
37.	Platforma trebuie să fie compatibilă cu standardele de criptare și protecție a datelor, asigurând confidențialitatea și integritatea datelor transmise și stocate, folosind metode de criptare de nivel înalt, cum ar fi AES-256 pentru datele stocate și TLS pentru datele transmise.
38.	Platforma trebuie să sprijine utilizarea de echipamente și infrastructuri de rețea non-proprietare, oferind suport pentru switch-uri, servere și alte componente de la diferiți furnizori, asigurând o soluție scalabilă și flexibilă, fără constrângeri legate de furnizorii de echipamente.
39.	Platforma trebuie să permită actualizarea și extinderea facilă a funcționalităților și componentelor, permițând adaptarea la nevoile viitoare ale infrastructurii de securitate, fără a fi necesare modificări semnificative ale arhitecturii sau echipamentelor existente.

40.	Platforma trebuie să sprijine utilizarea de servere și stații de lucru conforme cu specificațiile de securitate impuse de standardele internaționale, asigurând că toate componentele hardware respectă cerințele de protecție și integritate impuse de normele de securitate cibernetică.

4.2.3. Monitorizarea și raportarea în timp real

Nr.	Cerință
41.	Platforma trebuie să permită monitorizarea și raportarea în timp real a datelor și evenimentelor colectate de la dispozitivele de monitorizare video, senzori de notificare/alarmare; precum și de la alte echipamente integrate.
42.	Platforma trebuie să includă funcționalități de raportare în timp real a evenimentelor critice, permițând operatorilor să seteze niveluri de prioritate pentru notificări și alerte, astfel încât incidentele importante să fie gestionate eficient.
43.	Platforma trebuie să includă funcționalități de raportare în timp real a evenimentelor critice, permițând operatorilor să seteze niveluri de prioritate pentru notificări și alerte, astfel încât incidentele importante să fie gestionate eficient.
44.	Platforma trebuie să permită generarea de rapoarte personalizabile, care să includă grafice, diagrame și statistici privind activitatea din trafic și starea sistemului.
45.	Platforma trebuie să permită crearea de rapoarte personalizate complexe care să coreleze date din multiple surse (video, control acces, ALPR) într-un singur raport coerent.
46.	Platforma trebuie să permită vizualizarea în timp real a fluxurilor video multiple pe ecrane dedicate, oferind operatorilor capacitatea de a monitoriza simultan mai multe locații, cu posibilitatea de a comuta între fluxuri video și de a ajusta setările de afișare
47.	Platforma trebuie să includă funcționalități de căutare avansată în arhivele video, permițând identificarea rapidă a incidentelor pe baza unor criterii predefinite (de ex., ora, locația, tipul incidentului).
48.	Platforma trebuie să permită operatorilor să configureze și să monitorizeze simultan multiple fluxuri video pe ecrane dedicate, asigurând astfel o supraveghere eficientă și continuă.
49.	Platforma trebuie să suporte crearea și gestionarea incidentelor în timp real, permițând înregistrarea și urmărirea fiecărui incident până la rezolvarea acestuia.
50.	Platforma trebuie să includă funcționalități de gestionare a amenințărilor care să permită definirea și activarea rapidă a procedurilor de răspuns predefinite în cazul incidentelor majore.
51.	Platforma trebuie să ofere capabilități avansate de analiză a incidentelor, permițând operatorilor să coreleze rapid informații din sisteme video, de control acces și ALPR pentru a reconstitui evenimentele.
52.	Platforma trebuie să permită partajarea rapidă a informațiilor și a înregistrărilor video cu alte agenții sau autorități relevante, asigurând astfel o coordonare eficientă în caz de incidente majore.
53.	Platforma trebuie să permită funcționalități de export și distribuire a rapoartelor și datelor critice, permițând generarea rapidă a dosarelor de incident și transmiterea acestora în formate standardizate (PDF, CSV, Excel) pentru analiză ulterioară.
54.	Platforma trebuie să includă capacități de vizualizare a datelor în format geografic, permițând supravegherea vizuală a incidentelor și activităților pe hărți interactive, cu opțiuni de filtrare pe baza locației sau a altor parametri specifici.
55.	Platforma poate să includă funcționalități de monitorizare stare entități (*camere video, camere ANPR fixe și mobile, dispozitive IoT, etc.*) pe hartă și să permită personalizarea acestora.
56.	Platforma poate să includă funcționalități de accesare fluxurilor video direct din interfața de reprezentare geografică.
57.	Platforma trebuie să permită integrarea cu soluții de raportare și analiză predictivă, permițând generarea de analize detaliate care să identifice tipare și să ofere predicții despre tendințele traficului și incidentele viitoare.
58.	Platforma trebuie să permită personalizarea rapoartelor și a notificărilor în funcție de utilizator sau rol, asigurând că operatorii primesc doar informațiile relevante pentru activitatea lor, evitând astfel supraîncărcarea cu date neesențiale.

59.	Platforma trebuie să ofere funcționalități avansate de monitorizare a sănătății sistemului, inclusiv detectarea proactivă a anomaliilor și recomandări automate pentru optimizarea performanței.

4.3. Cerințe față de arhitectură.

Această secțiune se concentrează pe cerințele arhitecturale ale platformei și pe capacitatea acesteia de a se integra eficient cu alte sisteme și soluții existente sau viitoare. Platforma trebuie să fie flexibilă, scalabilă și să permită integrarea ușoară a noi componente și tehnologii, oferind în același timp o operare robustă și sigură.

4.3.1. Arhitectură deschisă și modulară:

Nr	Cerință
60.	Platforma trebuie să aibă o arhitectură deschisă și modulară, care să permită integrarea nativă cu sisteme terțe, inclusiv camere video, senzori IoT, sisteme de control acces și soluții ALPR, fără a necesita dezvoltări suplimentare complexe.
61.	Platforma trebuie să fie posibil de instalat local (on-premises) pe infrastructura de procesare asigurată de beneficiar, fie că aceasta constă în servere fizice sau mașini virtuale.
62.	Platforma trebuie să permită integrarea cu diverse tipuri de servere, soluții de stocare și echipamente de rețea, fără a necesita hardware proprietar, asigurând astfel flexibilitate în implementare și costuri reduse.
63.	Platforma trebuie să fie compatibilă cu soluțiile de virtualizare (ex. VMware, Hyper-V) și să permită rularea eficientă a componentelor sale în medii virtualizate sau cloud.
64.	Platforma trebuie să sprijine o arhitectură de tip microservicii, permițând distribuirea sarcinilor de procesare și reducerea dependențelor între diferitele module.
65.	Platforma trebuie să includă un API extensiv și bine documentat, care să permită dezvoltarea de aplicații personalizate și integrarea cu soluții software existente (de ex., ERP, REC sau sisteme de analiză).
66.	Platforma trebuie să permită integrarea de noi funcționalități și module software prin intermediul API-urilor deschise și standardizate, asigurând astfel extinderea capacităților fără întreruperi.
67.	Platforma trebuie să ofere interfața de comunicare standardizate (ex. RESTful API) pentru a facilita integrarea cu diverse sisteme terțe și pentru a permite interoperabilitatea între soluții diferite.
68.	Platforma trebuie să suporte procesare GPU accelerată pentru decodarea eficientă a fluxurilor video de înaltă rezoluție, reducând necesarul de hardware.
69.	Platforma trebuie să permită configurarea și gestionarea centralizată a tuturor componentelor sale, printr-o interfață unică de administrare, care să ofere acces la toate funcționalitățile necesare pentru operare și mentenanță.
70.	Platforma trebuie să includă suport nativ pentru actualizări automate și gestionarea centralizată a versiunilor software pentru toate modulele native și dispozitivele conectate.
71.	Platforma trebuie să permită utilizarea oricărui tip de hardware compatibil ONVIF (camere video, NVR-uri etc.), fără a fi limitată la dispozitivele unui anumit producător.
72.	Platforma trebuie să includă capabilități native pentru migrarea datelor din alte sisteme VMS sau de control acces către noul sistem, reducând timpul și costurile asociate tranziției
73.	Platforma trebuie să permită configurarea centralizată, granulară a permisiunilor utilizatorilor la nivel de module și funcționalități, asigurând un control detaliat asupra accesului la resursele platformei.

4.3.2. Implementare distribuită.

Nr.	Cerință
74.	Platforma trebuie să sprijine o arhitectură distribuită, în care componentele software și hardware pot fi amplasate în locații geografice diferite, asigurând o operare eficientă și sincronizată în timp real, indiferent de distanțe, cu posibilitatea de a partaja resurse (camere, rapoarte, utilizatori) între locații în timp real.
75.	Platforma trebuie să sprijine distribuirea sarcinilor de procesare și stocare între site-uri diferite, asigurând echilibrul sarcinilor și evitarea suprasolicitării unor locații specifice.

76.	Platforma trebuie să permită gestionarea centralizată a tuturor componentelor distribuite, oferind o interfață unică pentru administrarea și monitorizarea întregii rețele.
77.	Platforma trebuie să permită sincronizarea automată a datelor și evenimentelor între toate locațiile, asigurând că informațiile sunt actualizate și accesibile în timp real în orice locație conectată.
78.	Platforma trebuie să asigure continuitatea operațională în toate locațiile prin implementarea de mecanisme de failover distribuite, care să permită preluarea automată a sarcinilor în cazul unei defecțiuni locale.
79.	Platforma trebuie să ofere suport pentru configurarea unui sistem de disponibilitate ridicată (HA), asigurând că serviciile critice sunt replicate și disponibile fără întreruperi în caz de defecțiuni hardware sau software.
80.	Platforma trebuie să permită extinderea facilă a infrastructurii distribuite prin adăugarea de cel puțin 10 site-uri noi (locații) și resurse, fără a afecta performanța globală a sistemului.
81.	Platforma trebuie să suporte extinderea facilă a infrastructurii distribuite prin adăugarea de cel puțin 20 site-uri noi (locații) și resurse, fără a afecta performanța globală a sistemului.
82.	Platforma trebuie să ofere mecanisme de unificare a datelor și evenimentelor, permițând agregarea acestora din multiple locații într-o platformă unificată de management.
83.	Platforma trebuie să asigure un model de operare distribuit, în care fiecare site poate funcționa independent, dar toate datele și evenimentele să fie centralizate și disponibile pentru vizualizare și analiză în timp real.
84.	Platforma trebuie să permită configurarea de politici de acces diferențiate pentru fiecare locație, asigurând un control granular al permisiunilor și accesului la datele distribuite.
85.	Platforma trebuie să permită operatorilor să acceseze și să controleze resursele din orice locație a sistemului distribuit, în funcție de drepturile lor de acces, prin intermediul unei singure interfețe unificate.
86.	Platforma trebuie să permită administrarea descentralizată a site-urilor, oferind posibilitatea configurării și gestionării locale a componentelor, dar cu raportarea și agregarea datelor la nivel central.
87.	Platforma trebuie să sprijine monitorizarea centralizată a performanței și securității tuturor locațiilor distribuite, cu generarea de rapoarte unificate care să includă date din toate site-urile conectate.
88.	Platforma trebuie să asigure un flux de date sigur și optimizat între toate locațiile, minimizând latențele și asigurând integritatea și confidențialitatea informațiilor transmise.
89.	Platforma trebuie să sprijine configurarea dinamică a resurselor, permițând ajustarea automată a alocării resurselor în funcție de nevoile fiecărei locații și de volumul de date procesat.
90.	Platforma trebuie să asigure compatibilitatea cu diverse topologii de rețea și configurații de conectivitate, permițând implementarea sa în medii variate, de la centre urbane la locații izolate.
91.	Platforma trebuie să suporte integrarea cu aplicații mobile care să permită operatorilor de securitate să vizualizeze camere, uși, alarme și rapoarte din întreaga implementare distribuită, indiferent de locația fizică.
92.	Platforma trebuie să ofere acces unificat la toate componentele /modulele de securitate (video, control acces, ALPR) printr-o singură interfață mobilă intuitivă.
93.	Platforma trebuie să permită streaming-ul și capturarea video live de pe dispozitivele mobile ale operatorilor, cu posibilitatea de partajare instantanee către centrul de comandă.
94.	Platforma mobilă trebuie să includă funcționalități de geolocalizare pentru urmărirea în timp real a poziției operatorilor pe teren pe hărți interactive.
95.	Platforma mobilă trebuie să ofere capabilități avansate de gestionare a incidentelor, inclusiv preluarea controlului, urmărirea sarcinilor și comunicarea cu părțile interesate
96.	Platforma mobilă trebuie să includă un sistem de mesagerie în aplicație pentru comunicare securizată între operatorii mobili și personalul din centrul de comandă.
97.	Platforma mobilă trebuie să ofere notificări push în timp real pentru alarme și evenimente critice, cu posibilitatea de filtrare și prioritizare.
98.	Platforma mobilă trebuie să permită controlul de la distanță al ușilor și porților, semafoarelor, inclusiv suprascrierea programelor de blocare și acordarea accesului de urgență.

99.	Platforma mobilă trebuie să ofere capabilități de căutare și redare a înregistrărilor video arhivate, cu opțiuni de filtrare avansată.

4.3.3. Cerințe de securitate.

Nr.	Cerință
100.	Platforma trebuie să asigure criptarea tuturor comunicațiilor între componentele sistemului, utilizând protocoale de securitate avansate (ex. TLS) pentru a preveni interceptarea datelor.
101.	Platforma trebuie să sprijine autentificarea utilizatorilor și dispozitivelor conectate prin metode sigure, cum ar fi autentificarea multi-factor (MFA) și certificarea digitală.
102.	Platforma trebuie să includă un mecanism nativ, centralizat de jurnalizare, pentru toate componentele si modulele platformei, care să înregistreze toate acțiunile utilizatorilor și evenimentele critice, incluzând accesările, modificările de configurare, incidentele de securitate și alertele generate.
103.	Platforma trebuie să permită generarea de jurnale detaliate pentru fiecare subsistem integrat, oferind informații despre momentul, utilizatorul, acțiunea și rezultatul fiecărui eveniment.
104.	Platforma trebuie să includă un mecanism de audit automat, care să monitorizeze activitățile administratorilor și utilizatorilor cu privilegii ridicate, pentru a detecta orice tentativă de acces neautorizat sau abuz.
105.	Platforma trebuie să permită exportul și stocarea jurnale de audit și activitate într-un format standardizat (de exemplu, JSON, XML, CSV) pentru analiză externă și raportare.
106.	Platforma trebuie să permită integrarea cu soluții externe de jurnalizare și audit, inclusiv cu platforma guvernamentală de jurnalizare MLog, asigurând conformitatea cu cadrul normativ.
107.	Platforma trebuie să ofere un sistem de alertare automată bazat pe reguli personalizabile, care să notifice administratorii în cazul detectării unor activități anormale sau încercări de acces neautorizat în jurnalele de audit.
108.	Platforma trebuie să ofere suport pentru jurnalizarea externă către soluții SIEM (Security Information and Event Management) prin protocoale standard, pentru corelarea și analizarea evenimentelor de securitate la nivel enterprise.
109.	Platforma trebuie să includă funcțional pe baza de anumite evenimente sa declaseze fluxuri de lucru, indiferent de sursa evenimentului.
110.	Platforma trebuie să permită configurarea de politici de acces diferențiate, oferind control granular asupra permisiunilor și privilegiilor utilizatorilor în funcție de rolurile acestora.
111.	Platforma trebuie să asigure protecția împotriva atacurilor cibernetice în scop de detectare și prevenire a intruziunilor.
112.	Platforma trebuie să sprijine segmentarea rețelei și izolarea componentelor critice, minimizând riscul de propagare a amenințărilor în cazul unei breșe de securitate.
113.	Platforma trebuie să permită criptarea automată a fluxurilor media (video, audio, metadate) atât în tranzit, cât și în repaus, asigurând protecția datelor sensibile împotriva accesului neautorizat, fără a compromite performanța sistemului.
114.	Platforma trebuie să sprijine setarea criptării la nivel de cameră, permițând operatorilor să configureze criptarea individuală pentru fiecare dispozitiv, asigurând astfel o protecție suplimentară pentru fluxurile video și alte date transmise de camerele de supraveghere.
115.	Platforma trebuie să utilizeze chei de criptare generate aleatoriu, care să fie rotite periodic pentru a preveni atacurile de tip replay și pentru a asigura protecția pe termen lung a datelor.
116.	Platforma trebuie să permită managementul centralizat al cheilor de criptare, oferind administratorilor control complet asupra generării, distribuției și rotației cheilor, pentru a gestiona eficient securitatea criptografică a platformei.
117.	Platforma trebuie să fie conformă cu legislațiile naționale și internaționale privind protecția datelor, asigurând respectarea reglementărilor aplicabile, cum ar fi GDPR.
118.	Platforma trebuie să includă un modul de conformitate integrat, care să monitorizeze continuu starea sistemului și să genereze alerte în cazul unor neconformități detectate.
119.	Platforma trebuie să suporte mecanisme de audit și raportare, care să permită verificarea conformității cu standardele și reglementările de securitate aplicabile.

120.	Platforma trebuie să permită autentificarea utilizând protocoale moderne, inclusiv să fie integrată cu MPASS, asigurând un acces sigur și controlat la sistem.
121.	Platforma trebuie să permită definirea drepturilor și privilegiilor utilizatorilor, oferind un control detaliat asupra accesului la funcționalitățile platformei.
122.	Platforma trebuie să integreze soluții de management al identității și accesului (IAM), oferind o experiență de utilizare sigură și eficientă.
123.	Platforma trebuie să permită gestionarea centralizată a drepturilor și privilegiilor, oferind administratorilor capacitatea de a defini și revizui periodic accesul utilizatorilor.
124.	Platforma trebuie să includă funcționalități de audit și raportare a autentificărilor și activităților utilizatorilor, pentru a monitoriza și documenta accesul în sistem.
125.	Platforma trebuie să fie capabilă să detecteze și să prevină tentativele de acces neautorizat, declanșând alerte și blocând automat accesul în cazul unor activități suspecte.

4.3.4. Suport pentru extensii și inovație.

Nr.	Cerință
126.	Platforma trebuie să fie proiectată pe o arhitectură modulară, permițând adăugarea sau eliminarea de funcționalități și module fără a afecta stabilitatea și performanța sistemului.
127.	Platforma trebuie să suporte dezvoltarea și integrarea rapidă a modulelor suplimentare, permițând extinderea capacităților sale în funcție de cerințele operaționale și tehnologice emergente.
128.	Platforma trebuie să suporte implementarea de soluții personalizate pentru diferite scenarii de utilizare, asigurând flexibilitatea necesară pentru a răspunde cerințelor specifice ale fiecărei locații sau operațiuni.
129.	Platforma trebuie să ofere suport pentru API-uri deschise și standardizate, facilitând integrarea cu alte soluții software și hardware, precum și cu platforme terțe de securitate și monitorizare.
130.	Platforma trebuie să sprijine actualizările continue ale modulelor existente, asigurând compatibilitatea retroactivă și minimizând impactul asupra serviciilor în timpul procesului de upgrade.
131.	Platforma trebuie să fie compatibilă cu cele mai recente tehnologii de inteligență artificială (AI) și Machine Learning (ML), permițând implementarea de soluții avansate de analiză și predicție.
132.	Platforma trebuie să ofere suport pentru dezvoltarea și integrarea de soluții de automatizare a proceselor, reducând nevoia de intervenție manuală și îmbunătățind eficiența operațională.
133.	Platforma trebuie să suporte dezvoltarea și implementarea de algoritmi personalizați pentru analiza datelor, oferind posibilitatea de a optimiza soluțiile de securitate și monitorizare în funcție de nevoile lor specifice.
134.	Platforma trebuie să sprijine inovarea continuă prin integrarea facilă a noilor tehnologii și soluții, asigurând astfel că beneficiarul rămâne la curent cu cele mai recente dezvoltări din domeniul securității și monitorizării.
135.	Platforma trebuie să suporte integrarea cu platforme Cloud și de edge computing, oferind flexibilitate în gestionarea resurselor și scalarea capacităților în funcție de cerințele operaționale.
136.	Platforma trebuie să suporte integrarea cu soluții de Internet of Things (IoT).
137.	Platforma trebuie să permită gestionarea flexibilă a ciclului de viață al modulelor și funcționalităților, permițând upgrade-uri și actualizări iterative în funcție de cerințele operaționale și de securitate.

4.4. Evaluarea Performanței și Scalabilității.

Asigurarea unei performanțe constante și a posibilităților de extindere este crucială pentru a gestiona creșterea volumului de date și a cerințelor operaționale pe termen lung.

4.4.1. Scalabilitatea

Nr.	Cerință
138.	Platforma trebuie să permită extinderea de la 500 la cel puțin 5000 de camere prin adăugarea de resurse de procesare și licențe, fără necesitatea înlocuirii infrastructurii hardware existente.

139.	Platforma trebuie să permită extinderea de la 500 la cel puțin 20000 de camere prin adăugarea de resurse de procesare și licențe, fără necesitatea înlocuirii infrastructurii hardware existente.
140.	Platforma trebuie să fie proiectată pentru a fi non-hardware dependentă, permițând integrarea și operarea eficientă pe diverse tipuri de servere, dispozitive de stocare și echipamente de rețea, inclusiv cele existente.
141.	Platforma trebuie să sprijine extinderea prin adăugarea de noi locații și echipamente într-un mod modular, permițând implementarea progresivă și fără întreruperi a noilor resurse.
142.	Platforma trebuie să permită gestionarea centralizată a tuturor site-urilor și camerelor conectate printr-o singură interfață de management, asigurând o vizualizare unificată și coerentă a întregului sistem.
143.	Platforma trebuie să sprijine un model de implementare multi-site, permițând agregarea datelor și evenimentelor din multiple locații într-o platformă unificată, similar conceptului de federalizare.
144.	Platforma trebuie să permită distribuirea sarcinilor de procesare între multiple servere și locații, asigurând o performanță optimă și un timp de răspuns minim, indiferent de numărul de camere conectate.
145.	Platforma trebuie să sprijine integrarea cu sisteme terțe și tehnologii emergente, permițând extinderea capabilităților și funcționalităților fără constrângeri de compatibilitate.
146.	Platforma trebuie să permită adăugarea de noi funcționalități și module prin intermediul licențelor software suplimentare, fără necesitatea de a modifica infrastructura fizică existentă.
147.	Platforma trebuie să includă funcționalități avansate de balansare a încărcării și redundanță, pentru a asigura continuitatea operațională și prevenirea suprasolicitării resurselor.

4.4.2. Performanța

Nr.	Cerință
148.	Platforma trebuie să suporte procesarea a cel puțin 500 de fluxuri video simultane, fără a impacta calitatea imaginii sau viteza de procesare, cu posibilitatea de extindere la minim 5000 de fluxuri prin adăugarea de resurse de procesare și licențe suplimentare.
149.	Platforma trebuie să includă funcționalități de auto-optimizare, ajustând performanța în funcție de condițiile de operare și volumul de date procesat, pentru a menține un nivel constant de performanță.
150.	Platforma trebuie să permită monitorizarea continuă a performanței sistemului, cu generarea de rapoarte detaliate privind utilizarea resurselor, latențele și starea componentelor critice.
151.	Platforma trebuie să fie capabilă să gestioneze traficul de date între multiple locații, asigurând un flux de date sigur și rapid între site-uri și centrul de management.

4.4.3. Redundanță și recuperare în caz de dezastru

Nr.	Cerință
152.	Platforma trebuie să ofere mecanisme native de asigurarea redundanței la toate nivelurile critice ale sistemului (procesare, stocare, rețea), asigurând continuitatea operațiunilor chiar și în cazul unei defecțiuni majore.
153.	Platforma trebuie să sprijine replicarea datelor între multiple locații, permițând restaurarea rapidă a datelor în caz de dezastru și minimizând pierderile de informații.
154.	Platforma trebuie să permită configurarea automată a mecanismelor de failover, astfel încât, în cazul unei defecțiuni, sarcinile să fie preluate instantaneu de resursele de rezervă.
155.	Platforma trebuie să asigure compatibilitatea cu soluțiile de backup și recuperare în cloud, permițând protejarea și accesul la datele critice din orice locație.
156.	Platforma trebuie să includă funcționalități de monitorizare și raportare a stării sistemului de redundanță și backup, cu notificări automate în cazul detectării unor probleme.
157.	Platforma trebuie să sprijine planuri de recuperare în caz de dezastru testabile și documentate, permițând validarea periodică a capacității de restaurare a sistemului.
158.	Platforma trebuie să permită configurarea de proceduri automate pentru migrarea sarcinilor și datelor către alte locații în caz de necesitate, asigurând continuitatea operațională fără întreruperi.

5. CERINȚE FUNCȚIONALE ALE PLATFORMEI

5.1. Componenta de analiză a traficului rutier.

- Această secțiune definește cerințele pentru platforma de monitorizare și analiză a traficului rutier, care trebuie să asigure colectarea, procesarea și corelarea datelor din multiple surse, utilizând tehnologii avansate de edge computing și procesare server-based. Platforma trebuie să permită detecția automată a vehiculelor, analiza comportamentală, monitorizarea încălcărilor rutiere și furnizarea de informații detaliate pentru investigații și raportare.

- Funcționalități esențiale:

a. Procesare distribuită și analiză inteligentă:

–suport pentru procesare descentralizată (edge computing) la nivelul camerelor și dispozitivelor locale pentru optimizarea timpului de răspuns;

–procesare server-based scalabilă, capabilă să gestioneze volume mari de date și fluxuri video, fără degradarea performanței;

–detectare și clasificare automată a vehiculelor (număr de înmatriculare, tip, model, culoare, viteză) din surse multiple (camere ANPR, senzori, radare);

–analiză avansată a traficului pentru identificarea comportamentelor anormale și tendințelor de mobilitate.

b. Monitorizare și gestionare a incidentelor în timp real:

–identificare automată a încălcărilor rutiere, inclusiv depășirea vitezei, trecerea pe roșu, circulația interzisă, oprirea neregulamentară;

–generare de alerte și notificări automate, configurabile pe baza scenariilor definite de beneficiar;

–detecție și semnalare a vehiculelor de interes, prin sincronizare cu baze de date externe și liste de monitorizare;

–vizualizare în timp real și control asupra dispozitivelor de monitorizare, incluzând camere PTZ și senzori de trafic.

c. Investigații și analiză post-eveniment

–căutare avansată și reconstrucție vizuală a incidentelor, bazată pe metadate și arhive video;

–analiză forensică video, permițând corelarea evenimentelor din multiple surse pentru investigații detaliate;

–generare de rapoarte detaliate, incluzând tendințe de trafic, statistici privind incidentele și analize de risc;

–export și partajare a datelor relevante pentru utilizare în procese administrative, judiciare și de securitate.

d. Integrare și interoperabilitate extinsă

–expunere de API-uri standardizate, permițând integrarea cu sisteme terțe, inclusiv soluții de gestionare a sancțiunilor, control acces și infrastructură de transport inteligent;

–compatibilitate cu sisteme IoT și rețele de senzori, pentru îmbunătățirea preciziei analizelor de trafic;

–suport pentru protocoale și standarde deschise (ONVIF, REST API, MQTT), facilitând interoperabilitatea cu infrastructura existentă;

–integrare cu soluții de analiză big data și inteligență artificială, pentru optimizarea deciziilor bazate pe date.

Nr.	Cerință
159.	Platforma trebuie să asigure înregistrarea automată a tuturor vehiculelor care traversează puncte de monitorizare, utilizând resurse de tip edge-computing și/sau server-based. Datele colectate trebuie să includă imagini, data, ora și locația trecerii vehiculelor.
160.	Platforma trebuie să permită identificarea vehiculelor prin numărul de înmatriculare, cel puțin pentru vehicule din MD și spatiul UE.
161.	Platforma trebuie să permită vizualizarea și revizuirea în timp real a fluxului de vehicule, oferind operatorilor acces instantaneu la imagini și date colectate.
162.	Platforma trebuie să fie capabilă să detecteze automat vehicule, persoane și alte obiecte, utilizând algoritmi avansați de procesare a imaginilor. Obiectele trebuie clasificate cel puțin în funcție de dimensiune, formă, culoare, direcția de deplasare sau tipul vehiculului.

163.	Detecția și clasificarea automată trebuie să funcționeze în toate condițiile de iluminare (zi/noapte) și în condiții meteorologice variate, asigurând o acuratețe ridicată.
164.	Platforma trebuie să fie capabilă să genereze alerte automate în timp real atunci când sunt detectate evenimente de interes.
165.	Platforma trebuie să permită definirea, configurarea și ajustarea dinamică a regulilor pentru declanșarea alertelor, utilizând o interfață vizuală de tip drag-and-drop, care să faciliteze crearea și gestionarea scenariilor de securitate și monitorizare fără necesitatea unor intervenții tehnice complexe. Operatorii trebuie să poată configura condițiile specifice care declanșează automat alertele, combinând parametri precum, dar fără a se limita, tipul evenimentului, vehiculul sau meta datele acestuia, locația, ora, viteza sau comportamentul detectat.
166.	Platforma trebuie să permită escaladarea automată a incidentelor pe baza unui flux de lucru predefinit, direcționând notificările către operatorii relevanți și activând acțiuni automatizate, cum ar fi închiderea unei bariere, schimbarea culorii semaforului, alertarea unei patrule sau înregistrarea detaliată a incidentului. Scenariile trebuie să fie gestionabile dintr-o interfață unificată, permițând ajustări rapide și optimizări în timp real, astfel încât platforma să se adapteze dinamic la cerințele operaționale în schimbare, fără a necesita dezvoltări suplimentare sau costuri imprevizibile
167.	Platforma trebuie să includă capabilități de analiză comportamentală pentru a detecta automat activități sau comportamente neobișnuite în zona monitorizată cum ar fi, dar fără a se limita la: staționarea nejustificată, vehiculele care se deplasează în sens opus.
168.	Platforma trebuie să permită definirea și ajustarea regulilor comportamentale, permițând utilizatorilor să creeze scenarii personalizate de monitorizare și detectare.
169.	Platforma trebuie să includă un modul avansat de raportare, care să permită generarea de rapoarte detaliate cu privire la evenimente, vehicule și comportamente detectate, parvenite din diferite surse, inclusiv prin corelare cu evenimente parvenite din diferite module funcționale.
170.	Platforma trebuie să ofere funcționalități de analiză a comportamentului vehiculelor, permițând identificarea tiparelor de mișcare, urmărirea vehiculelor suspecte între multiple locații și predicția potențialelor amenințări.
171.	Platforma trebuie să ofere capabilități de vizualizare grafică și interactivă a datelor, permițând generarea de diagrame și alte reprezentări vizuale pentru analiza.
172.	Platforma trebuie să fie capabilă să detecteze automat încălcările regulilor de circulație cel puțin trecerea la culoarea roșie a semnalul semaforului, parcarea în zonă interzisă, deplasarea pe benzi specializate (cum ar fi banda destinată transportului public)
173.	Platforma trebuie să ofere funcționalități de capturare a imaginilor și înregistrărilor video relevante pentru fiecare încălcare, alături de datele de identificare ale vehiculului (număr de înmatriculare, viteză, data, ora, locația)
174.	Platforma trebuie să ofere alerte automate în caz de încălcări, notificând operatorii pentru a lua măsuri imediate.
175.	Platforma trebuie să ofere rapoarte statistice și analize asupra încălcărilor, cu opțiunea de a integra aceste date cu sistemele de gestionare a amenzilor.
176.	Platforma trebuie să fie capabilă să detecteze automat vehiculele suspecte sau care se află pe liste de interes (ex. vehicule furate) și să semnaleze acest lucru către operatori pentru investigare.
177.	Platforma trebuie să ofere suport pentru detectarea obiectelor sau vehiculelor staționare pentru perioade lungi de timp, alertând operatorii în caz de comportamente suspecte.
178.	Platforma trebuie să asigure actualizarea automată și manuală a listei de interes, cu posibilitatea de a adăuga sau elimina vehicule pe baza informațiilor furnizate de autorități.
179.	Platforma trebuie să permită integrarea cu bazele de date naționale și internaționale pentru a sincroniza și actualiza lista de interes în timp real.
180.	Platforma trebuie să permită urmărirea vehiculelor de interes în timp real, permițând vizualizarea traseului și a punctelor de trecere înregistrate.
181.	Platforma trebuie să fie capabil să genereze alerte instantanee atunci când vehiculele de interes sunt detectate, notificând imediat autoritățile competente sau operatorii responsabili.
182.	Platforma trebuie să ofere opțiuni de integrare cu sistemele de gestionare a contravențiilor.

5.2. Componenta de management video (VMS)

- Componenta de Management Video (VMS) este esențială pentru monitorizarea, înregistrarea și gestionarea fluxurilor video provenite de la camerele de supraveghere instalate în punctele de control al traficului rutier. Această secțiune detaliază funcționalitățile cheie pe care platforma trebuie să le includă pentru a asigura o monitorizare video eficientă și sigură.

Nr.	Cerință
183.	Platforma trebuie să permită agregarea fluxurilor video de la toate camerele de supraveghere conectate, oferind o vizualizare centralizată a acestora într-o interfață unificată.
184.	Platforma trebuie să suporte fluxuri video de la camere de diferite rezoluții și tipuri (ex. camere IP, PTZ, termice), asigurând compatibilitatea și interoperabilitatea între echipamente.
185.	Platforma VMS trebuie să includă capabilități native de criptare end-to-end pentru toate datele transmise și stocate, asigurând cel mai înalt nivel de securitate și confidențialitate
186.	Platforma trebuie să ofere capabilități avansate de protecție a confidențialității, inclusiv anonimizarea și mascarea în timp real a persoanelor în înregistrările video
187.	Platforma trebuie să permită configurarea fluxurilor video în funcție de nevoile operaționale, inclusiv setarea calității video, a cadrelor pe secundă și a modului de înregistrare (continuu, la detecție de mișcare, manual).
188.	Platforma trebuie să permită redarea în timp real și înregistrarea simultană a fluxurilor video, oferind opțiuni de control asupra parametrilor video (zoom, panoramare, înclinare) pentru camerele PTZ.
189.	Platforma trebuie să asigure sincronizarea automată a fluxurilor video cu datele de la alte sisteme (ex. ANPR, gestionarea incidentelor), pentru a permite corelarea informațiilor și o analiză eficientă.
190.	Platforma trebuie să permită crearea și gestionarea de grupuri de camere, oferind posibilitatea monitorizării simultane a mai multor fluxuri video într-o singură fereastră de vizualizare.
191.	Platforma trebuie să includă funcționalități de ajustare automată a parametrilor video în funcție de condițiile de iluminare și meteo, asigurând calitatea optimă a imaginilor înregistrate.
192.	Platforma trebuie să permită configurarea și gestionarea alarmei video, care să fie declanșată în funcție de detectarea unor evenimente specifice (ex. mișcare în zone restricționate).
193.	Platforma trebuie să permită arhivarea automată a fluxurilor video înregistrate, cu opțiuni de stocare pe termen scurt și lung, în funcție de necesitățile operaționale.
194.	Platforma trebuie să permită accesul rapid la arhivele video, cu funcționalități avansate de căutare pe baza criteriilor de timp, locație și tip de eveniment.
195.	Platforma trebuie să includă funcționalități de gestionare a spațiului de stocare, permițând administratorilor să aloce și să monitorizeze utilizarea capacității de stocare pentru fiecare cameră sau grup de camere.
196.	Platforma trebuie să permită setarea unor politici automate de curățare a arhivelor vechi, cu opțiuni de păstrare a înregistrărilor critice pentru perioade extinse de timp.
197.	Platforma trebuie să asigure criptarea înregistrărilor video stocate, pentru a proteja datele împotriva accesului neautorizat și a asigura conformitatea cu reglementările de securitate.
198.	Platforma trebuie să permită exportul înregistrărilor video în formate standardizate (ex. MP4, AVI) pentru utilizarea în investigații sau proceduri judiciare.
199.	Platforma trebuie să ofere funcționalități de redare a înregistrărilor video la diferite viteze, inclusiv redare cadru cu cadru și redare accelerată, pentru o analiză detaliată.
200.	Platforma trebuie să permită configurarea de alerte pentru administratorii de sistem în cazul în care spațiul de stocare atinge capacitatea maximă, pentru a preveni pierderea datelor.
201.	Platforma trebuie să permită arhivarea automată a fluxurilor video înregistrate, cu opțiuni de stocare pe termen scurt și lung, în funcție de necesitățile operaționale.
202.	Platforma trebuie să includă suport complet pentru camerele PTZ, permițând operatorilor să controleze mișcările camerelor (panoramare, înclinare, zoom) în timp real.
203.	Platforma trebuie să permită definirea unor tururi automate pentru camerele PTZ, permițând monitorizarea automată a zonelor critice conform unor trasee predefinite.

204.	Platforma trebuie să ofere funcționalități de detecție automată a mișcării și urmărirea automată a obiectelor în mișcare, utilizând camerele PTZ pentru a menține ținta în cadru.
205.	Platforma trebuie să permită configurarea de scenarii automate, unde camerele PTZ să reacționeze la evenimente detectate de alte sisteme (ex. detectarea unui vehicul pe lista de interes).
206.	Platforma trebuie să asigure compatibilitatea cu camere PTZ de la diferiți producători, permițând integrarea ușoară a noilor echipamente în infrastructura existentă.
207.	Platforma trebuie să ofere opțiuni de configurare a parametrilor PTZ direct din interfața de utilizator, inclusiv setarea zonelor de interes și a limitelor de mișcare.
208.	Platforma trebuie să permită configurarea de zone de protecție, în care mișcarea detectată de camerele PTZ să declanșeze automat alarme sau notificări.
209.	Platforma trebuie să includă funcționalități de diagnosticare și întreținere pentru camerele, oferind informații despre starea și funcționarea echipamentelor.
210.	Platforma trebuie să permită detectarea automată a mișcării și clasificarea obiectelor pe baza dimensiunii, vitezei și comportamentului acestora, oferind alerte în timp real pentru activitățile suspecte.
211.	Platforma trebuie să fie capabilă să analizeze activitatea pietonală și rutieră, generând rapoarte și statistici cu privire la fluxurile de persoane și vehicule, în scopul optimizării securității și gestionării traficului.
212.	Platforma trebuie să permită integrarea cu sisteme de tip BodyCam, inclusiv cele produse de Motorola, fără a necesita dezvoltări suplimentare, ci doar prin adăugarea de licențe dedicate. Sistemul trebuie să asigure recepția, gestionarea și analiza înregistrărilor video provenite de la dispozitivele BodyCam, oferind suport pentru clasificarea automată a evenimentelor, recunoaștere facială și analiză comportamentală, integrându-se nativ în fluxul de lucru al platformei.
213.	Platforma trebuie să includă funcționalități avansate de integrare cu soluțiile BodyCam de la Motorola, permițând recepția, stocarea, gestionarea și analiza înregistrărilor video provenite de la aceste dispozitive. Integrarea trebuie să fie realizată nativ, fără necesitatea dezvoltărilor suplimentare, și să suporte adăugarea de licențe dedicate. Oferta trebuie să includă cel puțin licențele necesare pentru integrarea și utilizarea a minimum 50 de camere BodyCam sau 50 de utilizatori, asigurând interoperabilitate completă cu sistemele de management video și fluxurile de analiză ale platformei.

5.3. Analiza video avansată.

- Analiza video avansată reprezintă un element fundamental în soluțiile moderne de securitate și monitorizare, permițând procesarea inteligentă a fluxurilor video pentru detectarea, clasificarea și corelarea evenimentelor în timp real și post-eveniment. Această tehnologie îmbunătățește considerabil capacitatea sistemelor de supraveghere de a identifica rapid incidente relevante, reducând volumul de date pe care operatorii trebuie să-l analizeze manual și accelerând procesul decizional.

- Conceptul de analiză video avansată presupune utilizarea algoritmilor specializați de procesare a imaginilor, care permit detectarea obiectelor și persoanelor, analiza comportamentală, recunoașterea vehiculelor și a numerelor de înmatriculare (ANPR), precum și corelarea informațiilor provenite din multiple surse. Această tehnologie permite filtrarea și căutarea forensică, facilitând identificarea rapidă a înregistrărilor relevante pe baza unor criterii specifice, precum atribute vizuale, trasee de deplasare, interacțiuni între elemente monitorizate sau evenimente anormale.

- Un alt aspect important al analizei video avansate este capacitatea de corelare a evenimentelor prin procesarea și indexarea automată a fluxurilor video, permițând identificarea tendințelor și a comportamentelor repetitive. Acest lucru se realizează prin generarea și utilizarea metadatelor extrase automat, cum ar fi locația, timpul, caracteristicile obiectelor și acțiunile detectate, facilitând integrarea cu alte sisteme de gestionare a incidentelor și securității.

- Edge computing și procesarea server-based joacă un rol esențial în analiza video avansată, permițând distribuirea sarcinilor de procesare între dispozitivele de captură (camere și senzori) și infrastructura centralizată. Acest model de procesare combinată optimizează timpul de răspuns și reduce încărcarea rețelei, permițând analize rapide și eficiente fără a compromite performanța sistemului.

- Platforma trebuie să ofere un cadru scalabil și modular, capabil să gestioneze volume mari de date video, fără a afecta performanța sau fiabilitatea infrastructurii. De asemenea, trebuie să includă interfețe intuitive, care permit navigarea rapidă prin înregistrările video, generarea de rapoarte detaliate și configurarea scenariilor de analiză.

- Prin utilizarea acestor tehnologii, analiza video avansată devine un instrument strategic pentru monitorizarea proactivă, investigarea rapidă a incidentelor și optimizarea procesului de luare a deciziilor, oferind autorităților un control eficient asupra securității și gestionării situațiilor critice.

Nr.	Cerință
214.	Platforma trebuie să includă capabilități de analiză video avansată, utilizând tehnologii emergente pentru detectarea comportamentului suspect și recunoașterea automată a obiectelor, cu specializări dedicate pentru: Analiza vehiculelor în trafic (ANPR) – recunoașterea automată a numerelor de înmatriculare, clasificarea vehiculelor, detectarea încălcărilor rutiere și generarea de alerte în timp real. Platforma trebuie să permită monitorizarea mai multor benzi de circulație simultan. Analiză Public-Safety (Investigație) – detectarea și investigarea comportamentelor suspecte și anomaliilor în spații publice, incluzând analiza obiectelor și persoanelor, identificarea riscurilor potențiale și generarea de rapoarte detaliate pentru investigații ulterioare. Ambele specializări trebuie să fie integrate într-o interfață unificată, oferind monitorizare în timp real și suport pentru investigarea și raportarea evenimentelor.
215.	Platforma trebuie să includă algoritmi avansați de analiză, bazați pe tehnologii AI specializate, pentru procesarea și interpretarea automată a datelor video. Platforma trebuie să utilizeze modele de învățare profundă (Deep Learning) și algoritmi de procesare computerizată a imaginilor pentru detecția, clasificarea și corelarea evenimentelor, asigurând o precizie ridicată în analiza comportamentală, identificarea anomaliilor și extragerea metadatelor relevante.
216.	Platforma trebuie să permită configurarea de reguli personalizate de analiză, permițând identificarea unor scenarii specifice de risc (*ex. părăsirea unui obiect într-o zonă publică*).
217.	Platforma trebuie să sprijine analiza video retrospectivă, oferind funcționalități de căutare în arhivele video pe baza tiparelor sau comportamentelor definite de utilizatori.
218.	Platforma trebuie să includă capacități avansate de căutare multi-cameră, permițând identificarea rapidă a persoanelor și vehiculelor de interes folosind filtre precum recunoașterea facială, similitudinea aspectului, îmbrăcăminte, culoare.
219.	Platforma trebuie să ofere funcționalități de recunoaștere a numerelor de înmatriculare (ANPR) pentru identificarea și urmărirea vehiculelor specifice în înregistrările video de la multiple camere.
220.	Platforma trebuie să permită configurarea de alerte în timp real bazate pe reguli, inclusiv recunoașterea facială, traversarea liniilor, vehicule, persoane de interes și numărarea obiectelor
221.	Platforma trebuie să ofere capabilități de gestionare a cazurilor, permițând organizarea activelor video specifice investigațiilor într-un singur fișier de caz și facilitând colaborarea dinamică.
222.	Platforma trebuie să includă funcționalități de analiză cantitativă a datelor video, oferind vizualizări intuitive sub formă de hărți de căldură și tablouri de bord pentru obținerea de informații operaționale acționabile.
223.	Platforma trebuie să suporte atât procesare video continuă în timp real, cât și analiză la cerere pentru multiple camere selectate.
224.	Platforma trebuie să accepte o rezoluție minimă de 480p și să permită procesarea fluxurilor video la rezoluții superioare (720p, 1080p) pentru îmbunătățirea distanței de detecție și acurateței. Rezoluția maximă acceptată trebuie să fie 4K.
225.	Platforma trebuie să permită analiza fluxurilor video cu o rată minimă de cadre de 8 FP.
226.	Platforma trebuie să permită analiza fluxurilor video provenite de la camere termice, acceptând o rezoluție minimă de QVGA (320 x 240 pixeli) și suportând fluxuri video la rezoluții superioare pentru îmbunătățirea distanței de detecție și a acurateței. De asemenea, platforma trebuie să permită procesarea fluxurilor video cu o rată minimă de cadre de 8 FPS.
227.	Platforma trebuie să utilizeze tehnologie bazată pe Deep Learning pentru detectarea și clasificarea automată a țintelor, asigurând identificarea precisă a următoarelor tipuri de obiecte, dar fără a se limita:

	• **Persoană**: În picioare, căzută sau întinsă pe sol; • **Transport pe două roți**: Motocicletă, bicicletă; • **Vehicul**: Autoturism, furgonetă/dubă, autobuz, camion; • **Obiect**: Genți, valize, rucsacuri, cutii, poșete; • **Fum și foc**: Detectarea fumului și a incendiilor;
228.	Platforma trebuie să fie capabilă să detecteze și să ignore automat obiectele care nu sunt relevante pentru procesul de analiză, inclusiv: Nori, Păsări, Câini/Pisici, Vegetație, etc.
229.	Platforma trebuie să permită definirea și antrenarea unui model personalizat de detecție pentru obiecte specifice, care nu sunt incluse în categoriile predefinite. Pentru aceasta, clientul trebuie să poată furniza un set de câteva sute de imagini relevante ale obiectului dorit, pe baza cărora să fie generat și optimizat un model de detecție dedicat. Platforma trebuie să permită integrarea acestui model personalizat în fluxul standard de analiză și clasificare a obiectelor.
230.	Platforma trebuie să includă reguli analitice care permit detectarea în timp real a comportamentelor anormale sau a situațiilor de interes, dar fără a se limita: • Mișcare într-o zonă / Staționare prelungită – detectarea țintelor care se deplasează într-o zonă de interes pentru o durată definită de utilizator. • Traversare linie – detectarea țintelor care au traversat o linie definită de utilizator, într-o direcție specifică sau în orice direcție. • Grupare – detectarea unui grup dens de persoane (număr configurabil) într-o zonă de interes, pentru o durată definită de utilizator. • Densitate mulțime – detectarea unui număr configurabil de persoane într-o zonă de interes, pentru o durată definită de utilizator. • Obiect abandonat – detectarea unui bagaj (valiză, geantă, rucsac, poșetă) lăsat într-o zonă de interes pentru o durată definită de utilizator. • Protecția activelor – marcare manuală a unui obiect în câmpul vizual și generarea unei alerte la îndepărtarea acestuia. • Detecția căderii – detectarea unei persoane care cade și rămâne întinsă pe sol.
231.	Platforma trebuie să permită detectarea automată a incidentelor și încălcărilor de trafic, prin reguli analitice specifice: • Vehicul oprit – detectarea vehiculelor care staționează într-o zonă de interes pentru o durată definită de utilizator. • Depășirea vitezei – detectarea vehiculelor care traversează o linie cu o viteză mai mare decât valoarea definită de utilizator. • Sens opus de trafic – detectarea unui vehicul care circulă într-o direcție interzisă.
232.	Platforma trebuie să integreze algoritmi de recunoaștere facială, permițând identificarea automată a persoanelor de interes în fluxurile video în timp real sau înregistrate, pentru cel puțin 20 de camere.
233.	Platforma trebuie să includă capacități avansate de recunoaștere facială, permițând cel puțin identificarea unei persoane dintr-un flux video care corespunde unui individ aflat într-o listă de supraveghere.
234.	Platforma trebuie să permită integrarea cu Registrul de Stat la Populației (RSP) gestionat de Agenția Servicii Publice, asigurând extragerea automatizată a fotografiilor persoanelor anunțate în căutare din Registrul Informațiilor Criminalistice și Criminologice (RICC). Platforma trebuie să sincronizeze periodic datele, permițând actualizarea listei de supraveghere în timp real și utilizarea acestor informații pentru identificarea automată a persoanelor detectate în fluxurile video.
235.	Fiecare regulă de detecție trebuie să fie aplicabilă tipurilor de ținte relevante, iar utilizatorul trebuie să aibă posibilitatea de a selecta mai multe tipuri de ținte pentru fiecare regulă de detecție.
236.	Platforma trebuie să permită configurarea și administrarea eficientă a regulilor analitice, oferind posibilitatea de a executa operațiuni în bulk pentru activarea, dezactivarea și programarea simultană a mai multor reguli. Platforma trebuie să permită rularea oricărei combinații de reguli analitice pe aceeași cameră, fără restricții, și să ofere operatorului posibilitatea de a defini multiple zone de detecție per cameră.

237.	Platforma trebuie să permită calibrarea automată și manuală a fiecărei camere, asigurând conversia precisă a dimensiunilor obiectelor din pixeli în unități reale de măsură (metri/picioare) pentru diferite zone ale imaginii.
238.	Platforma trebuie să utilizeze tehnici avansate de învățare automată pentru a modela și actualiza continuu profilul comportamental al scenei, identificând tiparele normale de activitate în funcție de locație, interval orar și zilele săptămânii.
239.	Platforma trebuie să includă o perioadă inițială de antrenare ('training'), în care sistemul colectează date pentru definirea unui model de comportament normal. Durata acestei perioade trebuie să fie configurabilă de către utilizator.
240.	Platforma trebuie să permită ajustarea și rafinarea continuă a detecției de anomalii prin feedback utilizator, oferind posibilitatea de a eticheta evenimentele detectate ca relevante sau irelevante. Evenimentele marcate ca irelevante trebuie utilizate pentru optimizarea algoritmului și reducerea alertelor false.
241.	Platforma trebuie să re-învețe periodic comportamentul normal al scenei, asigurând adaptarea la schimbările de context și eliminarea deviațiilor temporare care nu reprezintă riscuri reale.
242.	Platforma trebuie să analizeze în timp real comportamentul țintelor detectate, utilizând parametri precum: • Prezența și persistența țintei în câmpul vizual al camerei; • Traseul de deplasare al țintei; • Dimensiunea și modificarea acesteia în timp; • Viteza și schimbările bruște de direcție.
243.	Platforma trebuie să analizeze relațiile dintre mai multe ținte prezente în scenă, evaluând: • Numărul de ținte și distribuția acestora în câmpul vizual al camerei; • Distanțele relative dintre ținte și detectarea unor aglomerări neobișnuite
244.	Platforma trebuie să genereze automat evenimente de anomalie, incluzând: • Un clip video care conține momentele relevante, cu câteva secunde înainte și după detectarea evenimentului; • Casete de delimitare (bounding boxes) asupra țintelor relevante; • O descriere clară a comportamentului anormal detectat.
245.	Platforma trebuie să permită configurarea sensibilității detecției de anomalii, permițând utilizatorilor să definească pragurile de generare a alertelor în funcție de tipul de obiect și frecvența evenimentelor detectate.
246.	Platforma trebuie să permită încărcarea fișierelor video din surse externe pentru analiza post-eveniment, permițând procesarea acestora în regim de investigații. Platforma trebuie să ofere aceleași capabilități analitice aplicabile fluxurilor video live, inclusiv recunoaștere facială, detectarea anomaliilor, clasificarea obiectelor și analiza comportamentală, asigurând astfel o investigare detaliată a evenimentelor înregistrate.
247.	Platforma trebuie să permită detectarea și urmărirea automată a vehiculelor în mișcare, utilizând capabilități de recunoaștere a numerelor de înmatriculare și a caracteristicilor vehiculului.
248.	Platforma trebuie să sprijine integrarea cu soluții terțe de analiză video, permițând extinderea capabilităților de detectare și recunoaștere în funcție de cerințele operaționale.
249.	Platforma trebuie să includă funcționalități de vizualizare și raportare a rezultatelor analizei video, oferind operatorilor informații detaliate și ușor de interpretat.
250.	Platforma trebuie să ofere suport pentru actualizarea continuă a algoritmilor de analiză, asigurând adaptarea la noi tipuri de amenințări sau comportamente suspecte.
251.	Platforma trebuie să permită analiza comportamentului persoanelor și obiectelor în spații publice, cu alertare automată pentru riscuri detectate.
252.	Platforma trebuie să fie capabilă să coreleze evenimente multiple, identificând modele de comportament periculos și incidente asociate.
253.	Platforma trebuie să fie capabilă să genereze alerte vizuale și sonore pentru orice comportament deviant detectat, inclusiv pentru obiecte abandonate.
254.	Platforma trebuie să permită integrarea cu alte sisteme de securitate și supraveghere, inclusiv senzori audio pentru corelarea incidentelor cu alte surse de date.

255.	Platforma trebuie să fie capabilă să detecteze mișcarea și să identifice obiecte de interes (vehicule, persoane, obiecte abandonate) cu o acuratețe de cel puțin 95%.
256.	Platforma trebuie să asigure analiza comportamentală automată, identificând anomalii, comportamente suspecte și încălcări de reguli, generând alerte instantanee.
257.	Platforma trebuie să detecteze automat comportamente suspecte, precum aglomerații neobișnuite, obiecte abandonate sau mișcări anormale.
258.	Platforma trebuie să genereze rapoarte detaliate privind incidentele detectate, inclusiv videoclipuri asociate, marcate temporal pentru o investigație ușoară.
259.	Platforma trebuie să permită operatorilor să vizualizeze simultan fluxuri video în timp real și arhive video pentru investigarea incidentelor, fără întreruperea funcționalității de monitorizare live.
260.	Platforma trebuie să permită căutarea avansată în arhivele video pe baza unor criterii precum: număr de înmatriculare, tipul vehiculului, comportament suspect, data și ora, obiect, îmbrăcăminte, etc.
261.	Platforma trebuie să permită configurarea și definirea zonelor de interes pentru fiecare flux video, permițând filtrarea mișcărilor și evenimentelor în aceste zone.
262.	Platforma trebuie să permită exportul de înregistrări video, în formate standardizate, pentru a fi utilizate în alte sisteme sau pentru investigare.
263.	Platforma trebuie să permită realizarea investigațiilor video fără configurarea prealabilă a regulilor analitice, oferind posibilitatea de a efectua căutări simultane pe una sau mai multe camere selectate dintr-o listă sau hartă interactivă. Căutările trebuie să fie realizate pe baza unui set de comportamente predefinite, incluzând: • Detectarea persoanelor, vehiculelor pe două roți (motociclete, biciclete) și a altor vehicule (autoturisme, dube, autobuze, camioane) în mișcare, într-un interval de timp definit de utilizator, fie în întregul câmp vizual (FOV), fie într-o zonă de interes (AOI). • Identificarea țintelor care traversează o linie într-o direcție specificată sau în orice direcție. • Detectarea grupurilor de persoane și a ocupării unei zone în funcție de un prag de densitate configurabil. • Identificarea vehiculelor staționate într-o zonă de interes pentru o perioadă definită. • Detectarea obiectelor adăugate (genți, rucsacuri, valize) care rămân într-o zonă pentru o durată stabilită. • Căutarea persoanelor cu atribute similare unei imagini de referință ("Search for Similar").
264.	Platforma trebuie să permită filtrarea avansată a rezultatelor căutării prin criterii de clasificare și caracteristici vizuale ale țintei, inclusiv culoarea vestimentației pentru partea superioară și inferioară a corpului, precum și atributele specifice ale vehiculelor sau obiectelor analizate. Platforma trebuie să permită căutarea țintelor într-un interval de timp flexibil, incluzând: • Căutare în ultimele N minute, ore sau zile (ex: ultimele 3 ore, ultimele 7 zile). • Căutare într-un interval de timp definit de utilizator (ex: între 1 ianuarie ora 08:00 și 10 ianuarie ora 18:00). • Căutare într-un interval recurent (ex: între 08:00 - 09:00, în fiecare zi între 1-10 ianuarie).
265.	Platforma trebuie să permită funcționalitatea de "Search for Similar Targets", oferind posibilitatea de a iniția căutări suplimentare în arhiva video pentru a identifica ținte identice sau similare cu o țintă detectată anterior. Această căutare trebuie să poată fi efectuată înregistrat pe aceeași cameră sau pe un grup de camere selectate, fără restricții operaționale.
266.	Platforma trebuie să permită utilizatorilor să efectueze căutări avansate utilizând algoritmi AI capabili să interpreteze cereri formulate în limbaj natural. Utilizatorii trebuie să poată introduce prompt-uri textuale descriptive, iar sistemul să genereze rezultate relevante pe baza analizei metadatelor și a conținutului video. Funcționalitatea trebuie să includă, dar fără a se limita la: • Interpretarea cererilor complexe, cum ar fi: „Caută un vehicul roșu care a trecut pe roșu ieri dimineață între 08:00 și 09:00" sau „Găsește persoanele care au stat mai mult de 5 minute lângă intrarea principală". • Corelarea automată a criteriilor de căutare, utilizând analiza avansată a datelor video pentru a extrage informații despre tipul obiectelor, comportamente și locație.

	• Sugestii și ajustări dinamice, permițând utilizatorilor să rafineze căutările prin feedback iterativ, fără a necesita cunoștințe tehnice avansate. • Compatibilitate cu toate tipurile de căutare existente, inclusiv identificarea persoanelor, vehiculelor, traseelor, încălcărilor de trafic și altor evenimente relevante.
267.	Platforma trebuie să permită reconstrucția secvențelor video pentru a investiga în detaliu incidentele și a înțelege pe deplin evenimentele.
268.	Platforma trebuie să includă reguli analitice pentru analiza statistică a diferitelor tipuri de ținte, oferind cel puțin următoarele funcționalități: • Numărarea țintelor care traversează o linie virtuală definită de operator, cu capacitatea de a distinge individual țintele dintr-un grup (ex: dacă un grup de 4 persoane traversează linia, Platforma trebuie să înregistreze corect 4 intrări, nu 1). • Calcularea vitezei medii a vehiculelor care traversează o linie virtuală, permițând analiza comportamentului rutier în zonele monitorizate.
269.	Platforma trebuie să ofere statistici detaliate privind evenimentele generate în sistem pe o perioadă definită, suportând agregarea datelor în funcție de cameră, dispozitiv sau sursă, pe intervale de timp configurabile (ore, zile, săptămâni).
270.	Platforma trebuie să includă funcționalități avansate de filtrare și revizuire a evenimentelor video, permițând operatorilor să se concentreze doar pe evenimentele de interes (ex. comportamente suspecte, opriri neautorizate).
271.	Platforma trebuie să asigure compresie video H.264, H265, MPEG-4, MPEG-2, MJPEG pentru fluxurile video și MJPEG pentru capturile statice, optimizând stocarea și transmisia datelor.
272.	Platforma trebuie să permită detectarea automată a vehiculelor, inclusiv clasificarea acestora în funcție de tip autoturism, camion, motocicletă.
273.	Platforma trebuie să fie capabilă să recunoască comportamente neobișnuite sau activități suspecte, cum ar fi opriri neautorizate, schimbări bruște de direcție sau vehicule staționate în zone interzise.
274.	Platforma trebuie să asigure integrarea funcționalităților de recunoaștere a numerelor de înmatriculare (ANPR), cu o rată de acuratețe de cel puțin 98% în condiții normale de trafic și lumină, pentru cel puțin 125 fluxuri video simultan, într-o rezoluție minimă de 4k, fără a se limita la numărul de benzi sau direcția de deplasare.
275.	Platforma trebuie să fie capabilă să asigure determinarea vitezei deplasării vehiculelor în timp real, asigurând o marjă de eroare cel mult 10%, confirmate prin rapoarte de testare.
276.	Platforma trebuie să asigure captarea și procesarea plăcuțelor de înmatriculare ale vehiculelor care se deplasează cu viteză minimă de 150 km/h, menținând o acuratețe de minimum 99%.
277.	Platforma trebuie să asigure capturarea și procesarea plăcuțelor de înmatriculare ale vehiculelor care se deplasează cu viteză minimă de 250 km/h, menținând o acuratețe de minimum 95%. pentru vehiculele care circulă cu viteze mai mari de 200 km/h.
278.	Platforma trebuie să permită căutări avansate pe baza meta-datelor aferente vehiculului, locației și timpului, facilitând investigarea incidentelor.
279.	Platforma trebuie să fie capabilă să detecteze și să recunoască automat în timp real marca, culoarea și modelul vehiculului (ex: BMW, Audi, Toyota), utilizând algoritmi avansați de clasificare vizuală.
280.	Platforma trebuie să includă funcționalități de înregistrare a vehiculelor identificate în componenta de analiză a traficului rutier.
281.	Platforma trebuie să permită indexarea automată a fluxurilor video înregistrate, organizând toate datele pe baza caracteristicilor detectate (ex. vehicule, obiecte, activități).
282.	Platforma trebuie să ofere funcționalități avansate de căutare în înregistrările video, permițând filtrarea evenimentelor pe criterii multiple (ex. culoare, dimensiune, tip de vehicul, direcție de deplasare).
283.	Platforma trebuie să ofere opțiuni de export al datelor și înregistrărilor video pentru investigarea suplimentară sau utilizarea în alte sisteme de analiză și raportare.
284.	Platforma trebuie să fie capabilă să recunoască automat fețele persoanelor, inclusiv să ofere opțiuni de comparare cu liste de persoane cunoscute sau suspecte.

5.4. Interfața programatică de aplicație (API)

Nr.	Cerință
285.	Platforma trebuie să ofere un API robust care să permită accesul programatic la datele și funcționalitățile platformei, care sa includă toate componentele si modulele platformei, facilitând integrarea cu alte sisteme și aplicații.
286.	Platforma trebuie să asigure autentificarea și autorizarea utilizatorilor care accesează API-ul.
287.	Platforma trebuie să permită accesul la API prin metode standard, cum ar fi RESTful services, pentru a asigura interoperabilitatea și ușurința în utilizare.
288.	Platforma trebuie să ofere documentație completă și actualizată pentru API, incluzând exemple de utilizare, descrierea endpoint-urilor și specificațiile tehnice.
289.	Platforma trebuie să permită monitorizarea și auditarea accesului la API, oferind administratorilor un control complet asupra activităților programatice efectuate prin intermediul acestuia.
290.	Platforma trebuie să asigure securitatea datelor transmise prin API, implementând criptarea datelor în tranzit și protecția împotriva atacurilor de tip injection sau man-in-the-middle.

5.5. Monitorizarea și gestionarea incidentelor

Nr.	Cerință
291.	Platforma trebuie să permită monitorizarea în timp real a incidentelor detectate de camerele de supraveghere, oferind o interfață dedicată pentru gestionarea și documentarea acestora.
292.	Platforma trebuie să ofere o interfață unificată de monitorizare, comandă și control pentru toate dispozitivele și senzorii conectați, fără a necesita integrări suplimentare cu sisteme terțe.
293.	Platforma trebuie să includă un motor de reguli capabil să analizeze și să coreleze automat mii de evenimente pe secundă, clasificându-le în incidente prioritizate.
294.	Platforma trebuie să ofere capabilități de vizualizare avansată, inclusiv hărți interactive în timp real și suport pentru videowall, pentru a îmbunătăți conștientizarea situațională a operatorilor.
295.	Platforma trebuie să includă funcționalități de gestionare completă a incidentelor, de la detectare și calificare până la rezolvare și analiză post-incident.
296.	Platforma trebuie să ofere capacități de automatizare a răspunsului pentru situații de rutină, reducând necesitatea intervenției manuale a operatorilor.
297.	Platforma trebuie să detecteze automat incidentele pe baza unor reguli și scenarii predefinite, generând alerte în timp real la declanșarea evenimentelor critice.
298.	Platforma trebuie să permită clasificarea automată a incidentelor în funcție de tip, severitate și locație, pentru a asigura prioritizarea corectă a intervențiilor.
299.	Platforma trebuie să includă fluxuri de lucru predefinite și personalizabile, structurate în etape multiple, care să ghideze operatorii printr-un proces clar și coerent de gestionare a incidentelor. Fiecare flux de lucru trebuie să fie compus dintr-o succesiune logică de stări, pași și decizii, incluzând acțiuni automatizate, validări intermediare, notificări și escaladări bazate pe criterii prestabilite. Platforma trebuie să permită definirea și ajustarea acestor procese, asigurând o abordare sistematică și eficientă pentru fiecare tip de incident, reducând astfel timpul de răspuns și eliminând erorile operaționale.
300.	Platforma trebuie să permită configurarea și gestionarea fluxurilor de lucru personalizate pentru gestionarea incidentelor, printr-o interfață intuitivă de tip drag-and-drop.
301.	Platforma trebuie să permită fiecărui departament sau organizație să definească, adapteze și optimizeze procesele operaționale, fără a necesita cunoștințe tehnice avansate. Utilizatorii trebuie să poată crea și modifica scenarii de intervenție, stabilind condiții, acțiuni și reguli de escaladare, asigurând o coordonare eficientă a resurselor și un timp de răspuns redus la incidente.
302.	Platforma trebuie să permită alocarea automată și manuală a resurselor necesare, cum ar fi personalul de patrulare/securitate și echipamentele, pentru a gestiona fiecare incident corespunzător.
303.	Platforma trebuie să ofere o interfață unificată pentru vizualizarea, monitorizarea și gestionarea în timp real a tuturor incidentelor, facilitând coordonarea centralizată.
304.	Platforma trebuie să permită documentarea completă a fiecărui incident, incluzând momentul, locația, acțiunile întreprinse și resursele alocate pentru gestionare.

305.	Platforma trebuie să genereze rapoarte detaliate post-incident, incluzând date despre cauze, intervenții și rezultate pentru fiecare incident gestionat.
306.	Platforma trebuie să fie capabilă să integreze date din multiple surse (camere video, senzori, alarme), corelând aceste informații pentru a oferi o imagine completă a incidentului.
307.	Platforma trebuie să permită escaladarea automată a incidentelor nerezolvate, alertând echipele de management sau autoritățile competente dacă timpul de răspuns depășește un anumit prag.
308.	Platforma trebuie să sprijine colaborarea între echipe și agenții de securitate, permițând partajarea informațiilor și resurselor între organizații în timpul gestionării incidentelor majore.
309.	Platforma trebuie să permită revizuirea și validarea manuală a incidentelor, oferind operatorilor posibilitatea de a adăuga note și comentarii la fiecare caz documentat.
310.	Platforma trebuie să ofere funcționalități de auditare a gestionării incidentelor, înregistrând toate acțiunile întreprinse de operatori în timpul monitorizării și investigării cazurilor.

6. SUPORT TEHNIC ȘI MENTENANȚĂ

Pentru a asigura continuitatea și performanța optimă a soluției implementate, furnizorul are responsabilitatea de a oferi servicii complete de suport tehnic, garanție și mentenanță pe o perioadă minimă de 3 ani.

Această perioadă include asigurarea funcționării corecte a soluției, intervențiile corective și preventive, actualizările periodice de software și firmware, precum și furnizarea pieselor de schimb, după caz, necesare pentru menținerea sistemului operațional.

Furnizorul trebuie să garanteze opțiuni flexibile de extindere a serviciilor de suport și mentenanță, oferind soluții scalabile pentru prelungirea perioadei de acoperire. De asemenea, suportul tehnic live și accesul la resursele de auto-servire, împreună cu un timp de intervenție rapid pentru probleme critice, sunt esențiale pentru a minimiza impactul defecțiunilor asupra funcționării soluției.

Serviciile de mentenanță preventivă și evaluările anuale ale stării sistemului sunt componente esențiale pentru prevenirea defecțiunilor neașteptate, iar furnizorul trebuie să ofere documentație detaliată pentru întreținerea corectă a sistemului. Astfel, se va asigura că soluția rămâne aliniată la cele mai bune practici și standarde de securitate.

Nr.	Cerință
311.	Furnizorul soluției va asigura servicii de suport tehnic, mentenanță și garanție de producător pentru soluția livrată pe o perioadă de minim 3 ani.
312.	
313.	Furnizorul va asigura instalarea si configurarea platformei cu adaptarea la fluxurile de lucru ale beneficiarului pe resursele de procesare puse la dispoziție de către beneficiar.
314.	Serviciile și angajamentele de mentenanță trebuie să includă toate activitățile necesare pentru a asigura funcționarea corectă a soluției, cum ar fi intervențiile corective, preventive și predictive, precum și asistența tehnică la distanță sau la fața locului, atunci când este necesar.
315.	Furnizorul trebuie să asigure actualizări periodice ale software-ului și firmware-ului pe întreaga perioadă de garanție, mentenanță și suport, pentru a asigura îmbunătățirea performanțelor soluției și remedierea eventualelor vulnerabilități de securitate.
316.	Furnizorul trebuie să garanteze disponibilitatea pieselor de schimb pentru echipamentele livrate, după caz, pe toată durata perioadei de mentenanță, astfel încât orice defect să fie remediat rapid, fără întreruperea funcționării sistemului.
317.	Timpul maxim de intervenție pentru remedierea unei defecțiuni critice nu trebuie să depășească 24 de ore de la raportarea incidentului, iar pentru problemele minore intervenția trebuie efectuată în termen de 48 de ore.
318.	Soluția trebuie să permită monitorizarea proactivă, astfel încât potențialele probleme să fie detectate și raportate înainte ca acestea să devină critice, minimizând astfel riscurile de întrerupere a serviciilor.
319.	Pe întreaga durată a contractului de mentenanță și suport, furnizorul trebuie să asigure accesul extins la suport tehnic, incluzând o linie directă și un portal online pentru gestionarea rapidă a solicitărilor.
320.	Soluția trebuie să includă mentenanță preventivă programată pentru a asigura funcționarea optimă a sistemului și pentru a reduce riscurile de defecțiuni sau întreruperi neașteptate.

321.	Furnizorul la solicitare poate să efectueze evaluări anuale ale sistemului, analizând toate componentele, setările de configurare şi starea generală a sistemului, pentru a se asigura că respectă cele mai bune practici şi standarde de securitate.
322.	Furnizorul trebuie să furnizeze documentaţie detaliată de mentenanţă şi ghiduri pentru întreţinerea regulată a sistemului, inclusiv intervalele şi procedurile recomandate de mentenanţă
323.	Soluţia trebuie să includă suport telefonic şi prin chat live în timpul programului de lucru pentru asistenţă la depanare, consultanţă tehnică şi ghidare în configurare. Suportul trebuie să fie disponibil prin telefon, portal online sau chat live.
324.	Suportul trebuie să includă diagnostic colaborativ, oferind echipei tehnice acces de la distanţă (cu autorizare) pentru diagnosticare, replicare a problemelor şi soluţionare.
325.	Furnizorul trebuie să clasifice incidentele pe niveluri de severitate (Critic, Ridicat, Mediu, Scăzut) şi să ofere timpi de răspuns corespunzători.
326.	Furnizorul trebuie să asigure acces la un portal de suport online pentru gestionarea cazurilor, urmărirea incidentelor, accesul la articole din baza de cunoştinţe şi alte resurse de auto-servire.
327.	Furnizorul trebuie să asigure acces la toate actualizările software (majore, minore şi patch-uri) şi la remediile urgente pentru probleme critice.
328.	Furnizorul trebuie sa ofere suport tehnic de instalare şi configurare a soluţiei livrate.
329.	Furnizorul va organiza minimum 5 sesiuni de instruire (3 pentru utilizatori finali, 2 pentru administratori), fiecare de 8 ore, cu materiale în limba română şi engleză.

SEMNĂTURILE PĂRŢILOR	
Administrator **Victor BACIU** _____ LŞ	**Director** **Ion BOTNARI** _____ LŞ