Anexa nr.1
la Specificația Tehnică deplină propusă
pentru soluția Software (Postul Central de Dirijare)

Matricea de conformitate conform cerințelor solicitate la caietul de sarcini pentru soluția Software

Cerințe tehnice solicitate	**Cerințe tehnice propuse**
Tabelul nr. 1: Cerințe generale pentru Postul Central de Dirijare Postul Central de Dirijare (PCD) reprezintă componenta centrală ce realizează colectarea, sistimatizarea, stabilirea încălcării contravenționale și urmare a validării înregistrarea acestora în Registrul unic al contravențiilor, dețintor al căruia este Beneficiarul. Arhitectura PCD trebuie să fie deplin compatibilă cu medii de tip CLOUD, asigurind o scalabilitate cel putin pe orizontala, in vederea majorarii capacitatii de procesare. PCD va fi formată cel puțin din două componente DB si App, cu respectarea celor mai bune practici. Furnizorul va asigura livrarea Soluției software, kit-ului de instalare și codului sursă a acesteia, cu cel puțin cu drepul de modificare, dezvoltare și extindere; PCD trebuie să fie capabilă să proceseze înregistrări de la cel puțin 250 de posturi de supraveghere, cu posibilitatea de extindere a numărului acestora; PCD trebuie să asigure funcționarea în regim HA – High availability (disponibilitate înaltă) precum si in regim de balansare a incarcaturii. PCD trebuie să ofere scalabilitate pe orizontală flexibilă, în vederea inclusiv de majorare a numărului unităților de monitorizare PCD trebuie să fie una modulară, și să permită extindere funcțională la necesitate. PCD trebuie să includă cel puțin următoarele module funcționale; 1. Modul de gestiune a utilizatorilor; 2. Modul de gestiune a unităților de supraveghere; 3. Modul de gestiune a evenimentelor (încălcări RCR); 4. Modul de evidență a traversărilor (Vehicle Passing List) 5. Modul de audit și jurnalizare;	**Produsul ofertat: _____** Postul Central de Dirijare (PCD) reprezintă componenta centrală ce asigura realizează colectarea, sistematizarea, stabilirea încălcării contravenționale și urmare a validării înregistrarea acestora în Registrul unic al contravențiilor, dețintor al căruia este Beneficiarul. Arhitectura PCD asigură deplin compatibilitatea cu medii de tip CLOUD, asigurind o scalabilitate cel putin pe orizontala, in vederea majorarii capacitatii de procesare. PCD asigură cel puțin din două componente DB si App, cu respectarea celor mai bune practici. Furnizorul va asigura livrarea Soluției software, kit-ului de instalare și codului sursă a acesteia cu dreptul de modificare, dezvoltare și extindere; PCD asiguă procesarea înregistrări de la cel puțin 250 de posturi de supraveghere, cu posibilitatea de extindere a numărului acestora; PCD asigură funcționarea în regim HA – High availability (disponibilitate înaltă) precum si in regim de balansare a încărcăturii. PCD oferă scalabilitate pe orizontală flexibilă, în vederea inclusiv de majorare a numărului unităților de monitorizare **PCD este unu modular, și permite extinderea funcțională la necesitate.** **PCD include următoarele module funcționale;** **1. Modul de gestiune a utilizatorilor;** 2. Modul de gestiune a unităților de supraveghere; 3. Modul de gestiune a evenimentelor (încălcări RCR); 4. Modul de evidență a traversărilor (Vehicle Passing List)

6. Modul de raportare şi statistică; 7. Modul de gestiune alerte şi notificări; 8. Modul de procesare offline. Sistemul va permite accesarea funcţiilor Sistemului doar după autentificarea cu succes a utilizatorului. Sistemul va oferi suport pentru cel puţin următoarele metode de autentificare: în bază de ID şi parolă; prin intermediul serviciului electronic guvernamental de autentificare şi control al accesului - MPass Sistemul va permite utilizatorilor schimbarea parolelor individuale, inclusiv după prima autentificare PCD trebuie să includă interfeţe programabile (API-soap/xml sau openAPI) întru integrarea cu unităţile de supraveghere. Sistemul va permite gestionarea parametrilor de sistem din interfata utilizator. Pentru perioada de garanţie a proiectului furnizorul va asigura înlăturarea erorilor şi deficienţelor de sistem pentru a asigura buna funcţionare a acestuia **Tabelul nr. 2: Cerinţe pentru Modulul de gestiune a utilizatorilor** Modulul va asigura posibilitatea de gestiune centralizată a utilizatorilor sistemului, inclusiv cel puţin creare/modificare/suspendare/blocare; Modulul va permite gestiunea granulară a drepturilor de acces la toate obiectele Sistemului şi operaţiunile posibile asupra acestora (ex. entităţi de business, proprietăţi ale entităţilor de business, forme, meniuri, rapoarte, operaţiuni de creare / citire / actualizare / eliminare). Drepturile de acces la interfaţa utilizator şi înregistrările bazei de date vor fi definite de rolul aferent utilizatorului sau explicit pentru fiecare utilizator în parte Metoda de autorizare în cadrul Sistemului se va baza pe principiul „este interzis tot ce nu este explicit permis”. Modulul va asigura funcţional pentru resetarea parolei de acces a utilizatorilor Modulul va asigura crearea informaţiei de profil aferentă utilizatorilor (spre ex. ID, nume,.prenume, instituţie, email, telefon de contact, etc.) În cadrul profilurilor utilizatorilor se vor putea gestiona următoarele categorii de date: • nume, prenume utilizator; • adresă Email şi telefon de contact; • login de acces; • parolă de acces;	5. Modul de audit şi jurnalizare; 6. Modul de raportare şi statistică; 7. Modul de gestiune alerte şi notificări; 8. Modul de procesare offline. Sistemul permite accesarea funcţiilor Sistemului doar după autentificarea cu succes a utilizatorului. Sistemul oferă suport pentru cel puţin următoarele metode de autentificare: în bază de ID şi parolă; prin intermediul serviciului electronic guvernamental de autentificare şi control al accesului - MPass Sistemul permite utilizatorilor schimbarea parolelor individuale, inclusiv după prima autentificare PCD include interfeţe programabile API-soap/xml întru integrarea cu unităţile de supraveghere. Sistemul permite gestionarea parametrilor de sistem din interfata utilizator. Pentru perioada de garanţie a proiectului garantăm înlăturarea erorilor şi deficienţelor de sistem pentru a asigura buna funcţionare a acestuia **Tabelul nr. 2: Cerinţe pentru Modulul de gestiune a utilizatorilor** Modulul asigura posibilitatea de gestiune centralizată a utilizatorilor sistemului, inclusiv creare/modificare/suspendare/blocare; Modulul permite gestiunea granulară a drepturilor de acces la toate obiectele Sistemului şi operaţiunile posibile asupra acestora (ex. entităţi de business, proprietăţi ale entităţilor de business, forme, meniuri, rapoarte, operaţiuni de creare / citire / actualizare / eliminare). Drepturile de acces la interfaţa utilizator şi înregistrările bazei de date sunt definite de rolul aferent utilizatorului si explicit pentru fiecare utilizator în parte. Metoda de autorizare în cadrul Sistemului se bazează pe principiul „este interzis tot ce nu este explicit permis”. Modulul asigura funcţional pentru resetarea parolei de acces a utilizatorilor Modulul asigura crearea informaţiei de profil aferentă utilizatorilor (spre ex. ID, nume,.prenume, instituţie, email, telefon de contact, etc.) În cadrul profilurilor utilizatorilor se pot gestiona următoarele categorii de date: • nume, prenume utilizator; • adresă Email şi telefon de contact;

• strategie de autentificare (utilizator+parolă, semnătură electronică/semnătură) • cont activ/dezactivat; • perioadă de valabilitate a accesului; • alte date relevante. Sistemul va deține vizualizări și rapoarte privind drepturile de acces existente în Sistem; Modulul va asigura opțiuni de filtrare sau cautare după diferite criterii; Toate evenimentele cu privire la autentificarea în sistem (cu succes, sau eșuată) vor fi înregistrate în jurnalele de audit și logare evenimente. **Tabelul nr. 3: Cerințe pentru Modulul de gestiune a posturilor de supraveghere** Modulul va asigura evidența și gestiunea posturilor de supraveghere și a componentelor acestora Modulul va asigura capacitate de gestiune individuală a unităților de supraveghere, și/sau a grupurilor de unități Modulul trebuie să includă interfețe programabile (API-soap/xml) întru integrarea cu posturile/unitățile de supraveghere. Modulul va deține un mecanism de autentificare și autorizare a unităților de supraveghere, în componenta API, cel puțin în bază de IP și cheie de acces Componenta API trebuie să includă cel puțin următoarele interpelări: sincronizare nomenclatoare; înregistrarea evenimentelor cu privire la încălcări; înregistrarea traversărilor Setul de date pentru înregistrarea evenimentelor va include cel puțin: 1. PassingId 2. VehicleNumber 3. VehicleNumberImage 4. PlateType 5. PlateRecognitionValidity 6. VehicleCountryCode 7. VenicleType 8. VehicleColor 9. VehicleImages: list of images 10. Violations – lista incalcarilor 10.1. Article 10.2. ArticleChapter	• login de acces; • parolă de acces; • strategie de autentificare (utilizator+parolă, semnătură electronică/semnătură) • cont activ/dezactivat; • perioadă de valabilitate a accesului; • alte date relevante. Sistemul deține vizualizări și rapoarte privind drepturile de acces existente în Sistem; Modulul asigura opțiuni de filtrare sau cautare după diferite criterii; Toate evenimentele cu privire la autentificarea în sistem (cu succes, sau eșuată) sunt înregistrate în jurnalele de audit și logare evenimente. **Tabelul nr. 3: Capacitățile Modulului de gestiune a posturilor de supraveghere** Modulul asigura evidența și gestiunea posturilor de supraveghere și a componentelor acestora Modulul asigura capacitate de gestiune individuală a unităților de supraveghere, și/sau a grupurilor de unități Modulul include interfețe programabile (API-soap/xml) întru integrarea cu posturile/unitățile de supraveghere. Modulul deține un mecanism de autentificare și autorizare a unităților de supraveghere, în componenta API, în bază de IP și cheie de acces. Componenta API include următoarele interpelări: sincronizare nomenclatoare; înregistrarea evenimentelor cu privire la încălcări; înregistrarea traversărilor Setul de date pentru înregistrarea evenimentelor include cel puțin: 1. PassingId 2. VehicleNumber 3. VehicleNumberImage 4. PlateType 5. PlateRecognitionValidity 6. VehicleCountryCode 7. VenicleType 8. VehicleColor 9. VehicleImages: list of images 10. Violations – lista incalcarilor

10.3. ViolationType 10.4. NormalSpeed 10.5. VehicleSpeed 11. Device 12. DeviceTimeStamp 13. Note Setul de date pentru înregistrarea traversărilor va include cel puțin: 1. PassingId 2. VehicleNumber 3. VehicleNumberImage 4. PlateType 5. PlateRecognitionValidity 6. VehicleCountryCode 7. VenicleType 8. VehicleColor 9. VehicleImage 10. Device 11. DeviceTimeStamp 12. Note Modulul va permite înregistrarea și gestionarea informației de profil a posturilor/unităților de supraveghere (spre ex: Organizatia, ID, numărul unităților de supraveghere, locația geografică, lista echipamente, tip monitorizare, numărul certificat de aprobare de model și numărul buletinului metrologic, data valabilității, codul IBAN, grupul de operatori pentru repartizare, etc.) Modulul va asigura prezentarea informației cu privire la statutul unității de supraveghere Modulul va asigura opțiuni de filtrare sau cautare dupa diferite criterii Modulul va furniza funcțional de vizualizare a informației cu privire la conexiunile existente; ID; statut conexiune; data creării/activării/dezactivării; deținător/titular/gestionar; etc. Modulul va furniza functional de alertate si neadmiterii inregistrarii evenimetelor de incalcarea RCR dupa expirarea sau dezactivarea unitatii de supraveghere Tabelul nr. 4: Cerințe pentru Modulul de gestiune a evenimentelor	10.1. Article 10.2. ArticleChapter 10.3. ViolationType 10.4. NormalSpeed 10.5. VehicleSpeed 11. Device 12. DeviceTimeStamp 13. Note Setul de date pentru înregistrarea traversărilor include : 1. PassingId 2. VehicleNumber 3. VehicleNumberImage 4. PlateType 5. PlateRecognitionValidity 6. VehicleCountryCode 7. VenicleType 8. VehicleColor 9. VehicleImage 10. Device 11. DeviceTimeStamp 12. Note Modulul permite înregistrarea și gestionarea informației de profil a posturilor/unităților de supraveghere (spre ex: Organizatia, ID, numărul unităților de supraveghere, locația geografică, lista echipamente, tip monitorizare, numărul certificat de aprobare de model și numărul buletinului metrologic, data valabilității, codul IBAN, grupul de operatori pentru repartizare, etc.) Modulul asigura prezentarea informației cu privire la statutul unității de supraveghere Modulul asigura opțiuni de filtrare sau cautare dupa diferite criterii Modulul furnizează funcțional de vizualizare a informației cu privire la conexiunile existente; ID; statut conexiune; data creării/activării/dezactivării; deținător/titular/gestionar; etc. Modulul furnizează functional de alertate si neadmiterii inregistrarii evenimetelor de incalcarea RCR dupa expirarea sau dezactivarea unitatii de supraveghere

Modulul va asigura înregistrarea tuturor evenimentelor generate automatizat de unitățile de supraveghere prin intermediul web-serviciilor (API); Modulul trebuie să asigure funcțional pentru gestionarea nomenclatoarelor sistemului. Spre exemplu articole, alineate, norme în conformitate cu codul contravențional aplicabile sistemului. Trebuie să asigure evidența tuturor evenimentelor cu privire la încălcările RCR Modulul trebuie să asigure vizualizarea listei de evenimente și a informației generale aferente acestora Modulul trebuie să asigure posibilitatea de accesare și gestionare individuală a fiecărui eveniment, precum și a fișei de acțiuni Modul va asigura consumul de informații din surse externe, în vederea stabilirii altor încălcări ale RCR (spre exemplu: valabilitatea RCA, Reviziei tehnice, E-vinieta), anume în procesul validării evenimentului Schimbul de date cu sursele externe va fi asigurată prin intermediul Platformei Guvernamentale de Interoperabilitate MConnect Modulul va asigura funcționalitatea de validare/transmitere sau rebutare a evenimentului/lor; Modulul va asigura posibilitatea de anulare a statutului de rebutare; Modulul va asigura posibilitatea de redactare/corectare manuală a informațiilor înregistrate, de către operator (spre exemplu: în caz de citire eronată sau eroare la citirea numărului de înmatriculare, adaugare/editare articole și normelor contravenționale, etc.) Toate acțiunile utilizatorilor aferente modificărilor și/sau redactărilor operate vor fi înregistrate în jurnalele de audit și logare evenimente Modulul trebuie să permită înregistrarea evenimentelor generate prin consum de date din surse externe, inclusiv în regim offline pre-programat; Urmare a procesului de validare Modulul va asigura inregistrarea în Registrul de evidență a contravențiilor, cauzelor contravenționale, a persoanelor care le-au săvârșit și punctelor de penalizare a evenimentului, prin interfețele API puse la dispoziție de către acesta; Modulul va asigura posibilitatea de filtrare/cautare flexibilă după diferite criterii; Tabelul nr. 5: Cerințe pentru Modulul de evidență a traversărilor Cerințe funcționale pentru Modulul de evidență a traversărilor (Vehicle Passing List)	Tabelul nr. 4: Capacitatea Modulului de gestiune a evenimentelor Modulul asigura înregistrarea tuturor evenimentelor generate automatizat de unitățile de supraveghere prin intermediul web-serviciilor (API); Modulul trebuie să asigure funcțional pentru gestionarea nomenclatoarelor sistemului. Spre exemplu articole, alineate, norme în conformitate cu codul contravențional aplicabile sistemului. asigură evidența tuturor evenimentelor cu privire la încălcările RCR Modulul asigure vizualizarea listei de evenimente și a informației generale aferente acestora Modulul asigură posibilitatea de accesare și gestionare individuală a fiecărui eveniment, precum și a fișei de acțiuni Modul asigura consumul de informații din surse externe, în vederea stabilirii altor încălcări ale RCR (spre exemplu: valabilitatea RCA, Reviziei tehnice, E-vinieta), anume în procesul validării evenimentului Schimbul de date cu sursele externe sunt asigurate prin intermediul Platformei Guvernamentale de Interoperabilitate MConnect Modulul asigura funcționalitatea de validare/transmitere sau rebutare a evenimentului/lor; Modulul asigura posibilitatea de anulare a statutului de rebutare; Modulul asigura posibilitatea de redactare/corectare manuală a informațiilor înregistrate, de către operator (spre exemplu: în caz de citire eronată sau eroare la citirea numărului de înmatriculare, adaugare/editare articole și normelor contravenționale, etc.) Toate acțiunile utilizatorilor aferente modificărilor și/sau redactărilor operate sut înregistrate în jurnalele de audit și logare evenimente. Modulul permite înregistrarea evenimentelor generate prin consum de date din surse externe, inclusiv în regim offline pre-programat; Urmare a procesului de validare Modulul asigura înregistrarea în Registrul de evidență a contravențiilor, cauzelor contravenționale, a persoanelor care le-au săvârșit și punctelor de penalizare a evenimentului, prin interfețele API puse la dispoziție de către acesta; Modulul asigura posibilitatea de filtrare/căutare flexibilă după diferite criterii; Tabelul nr. 5: Capacitățile Modulul de evidență a traversărilor Capacitățile funcționale a Modulul de evidență a traversărilor (Vehicle Passing

Modulul trebuie să asigure evidența într-o listă unică a tuturor traversărilor vehiculelor, din zona de monitorizare, înregistrate de către unitățile de supraveghere Înregistrarea cu privire la traversarea vehiculelor trebuie să conțină cel puțin informația de data și ora exactă a traversării, o poză; numărul de înmatriculare, locația, ID-ul unității de captare, viteza de deplasare (dupa caz), direcția de deplasare, tipul vehiculului (după caz). Modul va asigura consumul de informații din surse externe, în vederea stabilirii încălcărilor RCR (spre exemplu: valabilitatea RCA, Reviziei tehnice, E-vinieta), în regim offline pre-programat Schimbul de date cu sursele externe va fi asigurată prin intermediul Platformei Guvernamentale de Interoperabilitate MConnect În baza traversărilor înregistrate modulul va asigura verificarea și contrapunerea cu informația din Modulul gestiune alerte și notificări Sistemul va asigura mecanism de ștergere automată (pre-programată) a pozelor cu privire la traversări pentru înregistrările mai vechi de 3 luni de zile (parametru de termen configurabil) Modulul va oferi posibilitatea redactării/corectării manuale a informației cu privire la traversare, (spre exemplu: eroare la citire sau citire eronată a numărului de înmatriculare) Toate acțiunile utilizatorilor aferente modificărilor și/sau redactărilor operate vor fi înregistrate în jurnalele de audit și logare evenimente Modulul va sigura posibilitatea de filtrare și căutare flexibilă, după diferite criterii, inclusiv după date incomplete (spre exemplu; C%% 000; CK% %%0; %%% 123) Tabelul nr. 6: Cerințe pentru Modulul de audit și jurnalizare Cerințe funcționale pentru Modulul de audit și jurnalizare Sistemul va deține componente de audit și jurnalizare ce vor colecta și gestiona centralizat înregistrările de audit la nivelul fiecărui modul al Sistemului. Componenta de audit și jurnalizare va permite configurarea granulară a politicilor de audit. Sistemul va permite stabilirea politicilor de audit cel puțin la nivel de obiect / entitate de business și la nivel de eveniment. Modulul va asigura înregistrarea oricărui eveniment generat în cadrul proceselor de business. Orice eveniment generat în cadrul proceselor de business implementate vor fi jurnalizate și salvate în tabelele corespunzătoare ale Bazei de	List) Modulul asigură evidența într-o listă unică a tuturor traversărilor vehiculelor, din zona de monitorizare, înregistrate de către unitățile de supraveghere Înregistrarea cu privire la traversarea vehiculelor conține cel puțin informația de data și ora exactă a traversării, o poză; numărul de înmatriculare, locația, ID-ul unității de captare, viteza de deplasare (dupa caz), direcția de deplasare, tipul vehiculului (după caz). Modul asigura consumul de informații din surse externe, în vederea stabilirii încălcărilor RCR (spre exemplu: valabilitatea RCA, Reviziei tehnice, E-vinieta), în regim offline pre-programat Schimbul de date cu sursele externe se asigurată prin intermediul Platformei Guvernamentale de Interoperabilitate MConnect În baza traversărilor înregistrate modulul asigura verificarea și contrapunerea cu informația din Modulul gestiune alerte și notificări Sistemul asigura mecanism de ștergere automată (pre-programată) a pozelor cu privire la traversări pentru înregistrările mai vechi de 3 luni de zile (parametru de termen configurabil) Modulul oferă posibilitatea redactării/corectării manuale a informației cu privire la traversare, (spre exemplu: eroare la citire sau citire eronată a numărului de înmatriculare) Toate acțiunile utilizatorilor aferente modificărilor și/sau redactărilor operate sunt înregistrate în jurnalele de audit și logare evenimente Modulul sigura posibilitatea de filtrare și căutare flexibilă, după diferite criterii, inclusiv după date incomplete (spre exemplu; C%% 000; CK% %%0; %%% 123) Tabelul nr. 6: Capacitățile Modulului de audit și jurnalizare Sistemul deține componente de audit și jurnalizare ce vor colecta și gestiona centralizat înregistrările de audit la nivelul fiecărui modul al Sistemului. Componenta de audit și jurnalizare permite configurarea granulară a politicilor de audit. Sistemul permite stabilirea politicilor de audit cel puțin la nivel de obiect / entitate de business și la nivel de eveniment. Modulul asigura înregistrarea oricărui eveniment generat în cadrul proceselor de business. Orice eveniment generat în cadrul proceselor de business implementate sunt jurnalizate și salvate în tabelele corespunzătoare ale Bazei

Date. Mecanismul de jurnalizare va fi dezvoltat în baza standardelor şi bunelor practici implementate în industrie Sistemul va livra funcționalități de configurare a strategiei de jurnalizare a evenimentelor de business, inclusiv: categoriile de evenimente de business supuse jurnalizării, perioada calendaristică de jurnalizare (determinată sau nedeterminată) etc Vor fi jurnalizate cel puțin următoarele categorii de evenimente: • autentificare utilizator; • deconectare utilizator; • adăugare/modificare/eliminare/accesare înregistrare; • evenimente de business specifice fluxurilor de lucru • sincronizarea cu sisteme informatice terțe; • generare/accesare raport; • interogări la baza de date; • alte evenimente de business specifice. Evenimentele jurnalizate vor salva următoarele categorii de date (în funcție de natura evenimentului jurnalizat: • identificatorul utilizatorului care a generat evenimentul; • categoria evenimentului jurnalizat; • momentul jurnalizării evenimentului; • modulul sistemului care a generat evenimentul de business; • înregistrarea afectată de evenimentul de business; • acțiunea efectuată de utilizator; • Adresa IP a sursei ce a inițiat evenimentul. Înregistrările de audit nu vor conține informație de business confidențială (ex. parole introduse la încercările eșuate). Pentru evenimentele business critice sau sensibile, jurnalizarea se va efectua în paralel utilizându-se Serviciul electronic guvernamental de jurnalizare - MLog Modulul va furniza funcționalitate de definire a evenimentelor de business critice care urmează a fi jurnalizate în paralel prin intermediul serviciului MLog. Componenta de audit şi jurnalizare va deține un mecanism de arhivare a înregistrărilor de audit istorice. Procesul de arhivare va putea fi parametrizat (frecvența, vechime date, format arhivare, destinație, etc.). Sistemul va putea genera automat notificări către persoanele responsabile la producerea anumitor evenimente de securitate, conform configurațiilor setate. Sistemul va permite fixarea versiunilor istorice ale datelor, ce vor fi considerate deosebit de senzitive.	de Date.Mecanismul de jurnalizare este dezvoltat în baza standardelor şi bunelor practici implementate în industrie Sistemul livrează funcționalități de configurare a strategiei de jurnalizare a evenimentelor de business, inclusiv: categoriile de evenimente de business supuse jurnalizării, perioada calendaristică de jurnalizare (determinată sau nedeterminată) etc Sunte jurnalizate următoarele categorii de evenimente: • autentificare utilizator; • deconectare utilizator; • adăugare/modificare/eliminare/accesare înregistrare; • evenimente de business specifice fluxurilor de lucru • sincronizarea cu sisteme informatice terțe; • generare/accesare raport; • interogări la baza de date; • alte evenimente de business specifice. Evenimentele jurnalizate salvează următoarele categorii de date (în funcție de natura evenimentului jurnalizat: • identificatorul utilizatorului care a generat evenimentul; • categoria evenimentului jurnalizat; • momentul jurnalizării evenimentului; • modulul sistemului care a generat evenimentul de business; • înregistrarea afectată de evenimentul de business; • acțiunea efectuată de utilizator; • Adresa IP a sursei ce a inițiat evenimentul. Înregistrările de audit nu conțin informații de business confidențială (ex. parole introduse la încercările eșuate). Pentru evenimentele business critice sau sensibile, jurnalizarea se efectuează în paralel utilizându-se Serviciul electronic guvernamental de jurnalizare - MLog Modulul va furniza funcționalitate de definire a evenimentelor de business critice care urmează a fi jurnalizate în paralel prin intermediul serviciului MLog. Componenta de audit şi jurnalizare deține un mecanism de arhivare a înregistrărilor de audit istorice. Procesul de arhivare poat fi parametrizat (frecvența, vechime date, format arhivare, destinație, etc.). Sistemul poate genera automat notificări către persoanele responsabile la

Modulul va asigura accesarea și procesarea comodă a evenimentelor log înregistrate, inclusiv filtrarea înregistrărilor după diferite criterii și exportul acestora în format uzual Tabelul nr. 7: Cerințe pentru Modulul de raportare şi statistică Cerințe funcționale pentru Modulul raportare și statistică Modulul va furniza mecanism de generare a rapoartelor predefinite și ad-hoc capabile să asigure o analiză sau evaluare pertinentă Modulul va deține cel puțin următoarele rapoarte predefinite: 1. Raport evenimente (posibilitatea selectării perioadei de timp și a locației) va conține cel puțin următoarea informație: ID-ul si denumirea locației; numărul total de evenimente captate în perioada selectată, clasificarea după tipul încălcării (viteză, marcaj, semafor), cîte din ele au fost validate, cîte rebutate și cîte în așteptare. 2. Raport de activitate a utilizatorilor (posibilitatea selectării perioadei de timp și a utilizatorului) va conține cel puțin următoarea informație: utilizator, Nume Prenume, evenimente prelucrate în perioada selectată, cîte din ele validate, cîte rebutate, cîte din ele modificate. 3. Raport traversări (posibilitatea selectării perioadei de timp și a locației) va conține cel puțin următoarea informație: ID-ul si denumirea locației; numărul total de traversări captate în perioada selectată, clasificarea mijloacelor de transport (autoturism, camion etc) Modulul va permite generarea rapoartelor si modelarea dinamica a acestora dupa principiu de Pivot Table Toate vizualizările și rapoartele din Sistem trebuie să poată fi imprimate pe formatul de pagină indicat. Sistemul trebuie să dimensioneze automat documentele de ieșire pentru a se încadra în formatul indicat de utilizator (ex. A2/3/4, portrait / landscape, etc.). Modulul trebuie să permită exportarea în format PDF (implicit) sau într-un fișier extern redactabil (XLS/XLSX, CSV). Generarea rapoartelor și accesarea informației în scopul analizelor de business nu trebuie să afecteze performanța operațională a Sistemului Modulul va jurnaliza toate evenimentele de generare și imprimare a rapoartelor și documentelor. Tabelul nr. 8: Cerințe pentru Modulul de gestiune alerte și notificări Cerințe funcționale pentru Modulul gestiune alerte și notificări	producerea anumitor evenimente de securitate, conform configurațiilor setate. Sistemul permite fixarea versiunilor istorice ale datelor, ce vor fi considerate deosebit de senzitive. Modulul asigura accesarea și procesarea comodă a evenimentelor log înregistrate, inclusiv filtrarea înregistrărilor după diferite criterii și exportul acestora în format uzual Tabelul nr. 7: Capacitatea Modulul de raportare și statistică Modulul furnizează mecanism de generare a rapoartelor predefinite și ad-hoc capabile să asigure o analiză sau evaluare pertinentă Modulul deține cel puțin următoarele rapoarte predefinite: 1. Raport evenimente (posibilitatea selectării perioadei de timp și a locației) conține cel puțin următoarea informație: ID-ul si denumirea locației; numărul total de evenimente captate în perioada selectată, clasificarea după tipul încălcării (viteză, marcaj, semafor), cîte din ele au fost validate, cîte rebutate și cîte în așteptare. 2. Raport de activitate a utilizatorilor (posibilitatea selectării perioadei de timp și a utilizatorului) conține următoarea informație: utilizator, Nume Prenume, evenimente prelucrate în perioada selectată, cîte din ele validate, cîte rebutate, cîte din ele modificate. 3. Raport traversări (posibilitatea selectării perioadei de timp și a locației) conține următoarea informație: ID-ul si denumirea locației; numărul total de traversări captate în perioada selectată, clasificarea mijloacelor de transport (autoturism, camion etc) Modulul permite generarea rapoartelor si modelarea dinamica a acestora dupa principiu de Pivot Table Toate vizualizările și rapoartele din Sistem sunt imprimate pe formatul de pagină indicat. Sistemul dimensioneze automat documentele de ieșire pentru a se încadra în formatul indicat de utilizator (ex. A2/3/4, portrait / landscape, etc.). Modulul permite exportarea în format PDF (implicit) sau într-un fișier extern redactabil (XLS/XLSX, CSV). Generarea rapoartelor și accesarea informației în scopul analizelor de business nu afectează performanța operațională a Sistemului Modulul va jurnaliza toate evenimentele de generare și imprimare a rapoartelor și documentelor.

Modulul va permite gestiunea alertelor și notificărilor cu privire la evenimente de interes Modulul va permite setarea și configurarea declanșatoarelor de alerte, în baza diferitor indicatori Modulul va permite crearea listei roșii (REDlist) care presupune posibilitatea de identificare a mijloacelor de transport de interes, în regim real de timp, la momentul traversării zonelor de monitorizare Modulul va asigura alertarea și notificarea utilizatorilor autorizați în cazul identificării evenimentelor de interes Înregistrarea cu privire la mijloacele de transport întroduse în lista roșie va conține cel puțin următorul set de date: 1. Număr de înmatriculare (cîmp obligatoriu) 2. Modelul mijlocului de transport (cîmp opțional) 3. Culoarea mijlocului de transport (cîmp opțional) 4. Motivul includerii (cîmp obligatoriu) 5. Inițiatorul (cîmp obligator) 6. Perioada (cîmp obligator) Alertele vor conține cel puțin următoarea informație: numărul de înmatriculare, poza mijlocului de transport, data, ora și locația fixării, inițiatorul precum și motivul întroducerii în lista roșie. Modulul va permite efectuarea căutărilor în lista mijloacelor de transport introduse după număr de înmatriculare sau perioadă de timp. Modulul va asigura funcționalitatea de notificare pentru cel puțin următoarele evenimente: 1. Traversarea zonei de monitorizare depășind viteza admisibilă cu mai mult de 40km/h (valoare configurabilă); 2. Depășirea vitezei de deplasare înregistrată la 2 sau mai multe posturi de supraveghere, într-o perioadă scurtă de timp (valoare configurabilă); 3. Exploatarea mijlocului de transport fără număr de îmnatriculare. Notificările vor conține cel puțin următoarea informație: numărul de înmatriculare (după caz), poza mijlocului de transport, data, ora și locația fixării Toate acțiunile utilizatorilor vor fi înregistrate în jurnalele de audit și logare. Tabelul nr. 9: Cerințe pentru Modulul de procesare offline C9 - Cerințe funcționale pentru Modulul de procesare offline Modulul reprezinta componenta software destinata procesarii offline in regim	Tabelul nr. 8: Capacitățile Modulului de gestiune alerte și notificări Modulul va permite gestiunea alertelor și notificărilor cu privire la evenimente de interes Modulul permite setarea și configurarea declanșatoarelor de alerte, în baza diferitor indicatori Modulul permite crearea listei roșii (REDlist) care presupune posibilitatea de identificare a mijloacelor de transport de interes, în regim real de timp, la momentul traversării zonelor de monitorizare Modulul va asigura alertarea și notificarea utilizatorilor autorizați în cazul identificării evenimentelor de interes.Înregistrarea cu privire la mijloacele de transport întroduse în lista roșie conține cel puțin următorul set de date: 1. Număr de înmatriculare (cîmp obligatoriu) 2. Modelul mijlocului de transport (cîmp opțional) 3. Culoarea mijlocului de transport (cîmp opțional) 4. Motivul includerii (cîmp obligatoriu) 5. Inițiatorul (cîmp obligator) 6. Perioada (cîmp obligator) Alertele conțin următoarea informație: numărul de înmatriculare, poza mijlocului de transport, data, ora și locația fixării, inițiatorul precum și motivul întroducerii în lista roșie. Modulul permite efectuarea căutărilor în lista mijloacelor de transport introduse după număr de înmatriculare sau perioadă de timp. Modulul asigura funcționalitatea de notificare pentru cel puțin următoarele evenimente: 1. Traversarea zonei de monitorizare depășind viteza admisibilă cu mai mult de 40km/h (valoare configurabilă); 2. Depășirea vitezei de deplasare înregistrată la 2 sau mai multe posturi de supraveghere, într-o perioadă scurtă de timp (valoare configurabilă); 3. Exploatarea mijlocului de transport fără număr de îmnatriculare. Notificările conține cel puțin următoarea informație: numărul de înmatriculare (după caz), poza mijlocului de transport, data, ora și locația fixării Toate acțiunile utilizatorilor sunt înregistrate în jurnalele de audit și logare. **Tabelul nr. 9: Capacitățile Modulul de procesare offline** Modulul reprezinta componenta software destinată procesarii offline in regim asyncron, pre-programat, a fluxurilor de date si evinimentelor inregistrate in

asyncron, pre-programat, a fluxurilor de date si evinimentelor inregistrate in sistem. Modulul va include functional de gestionare a fregventei/perioadei(scheduler) de declasare a sarcinei(task) de procesare in dependeta de actiunile ce necesita a fi realizate. Toate sarcinile declansate(tasks) vor rula idenpendent unul fata de altul intr-un regim asyncron. Toate sarcinile vor fi gestionate/procesate prin intermediul unei cozi de asteptare(queue) si executate segvential in ordinea prioritatii acestora. Modul va include functional de definire/gestionare a declansatoarelor(trigers) in baza unor valori/indicatori configurabili(spre exemplu generarea alertei privind depasirea vitezei de deplasare x km/h) UCP trebuie să includă modulul de interpelare componentelor/sistemelor externe (SOAP/XML) în scopul stabilirii contravenției (exemplu: RCA, Revizia Tehnica, etc.). Modulul va include functional de vizualizarii informatiei relevante cu privire la starea acestuia, cozii de asteptare, precum si statutelor declansatoarelor. VII.02 Cerințe Non-funcționale Arhitectura Sistemului trebuie să fie aliniată la necesitățile Beneficiarul ce țin de flexibilitatea și mentenabilitatea sistemului. Beneficiarul optează pentru o arhitectură deschisă, modulară, bazată pe componente interoperabile. Aceste principii trebuie să fie vizibile la toate nivelele arhitecturii sistemului. Tabelul nr. 10: Cerințe Non-funcționale ID Obligativitate Cerință Arhitectura sistemului trebuie să fie bazată pe standarde deschise. Arhitectura sistemului va fi de tipul client-server, organizată în cel puțin 3 nivele verticale(utilizator, aplicație, date) , divizate clar, astfel încât fiecare nivel superior să depindă doar de nivelul său inferior. Comunicarea între toate componentele sistemului se va face securizat, utilizând în acest scop interfețele interne ale componentelor sistemului Sistemul. Nivelul de prezentare Nivelul de prezentare este responsabil pentru asigurarea interacțiunii utilizatorului cu funcțiile de business ale Sistemului. Acest nivel de arhitectură gestionează modul în care utilizatorii accesează și utilizează funcțiile Sistemului atât în scop de business, cât și în scop administrativ. Sistemul urmează să fie accesat doar de către utilizatorii autorizați. Suplimentar, Sistemul va comunica cu alte sisteme ale Beneficiarul prin interfețe externe (cerințe relevante sunt stabilitate la capitolul „Interoperabilitate”).	sistem. Modulul include functional de gestionare a fregventei/perioadei(scheduler) de declasare a sarcinei(task) de procesare in dependeta de actiunile ce necesita a fi realizate. Toate sarcinile declansate(tasks) vor rula idenpendent unul fata de altul intr-un regim asyncron. Toate sarcinile sunt gestionate/procesate prin intermediul unei cozi de asteptare(queue) si executate segvential in ordinea prioritatii acestora. Modul include functional de definire/gestionare a declansatoarelor(trigers) in baza unor valori/indicatori configurabili(spre exemplu generarea alertei privind depasirea vitezei de deplasare x km/h) UCP include modulul de interpelare componentelor/sistemelor externe (SOAP/XML) în scopul stabilirii contravenției (exemplu: RCA, Revizia Tehnica, etc.). Modulul include functional de vizualizarii a informatiei relevante cu privire la starea acestuia, cozii de asteptare, precum si statutelor declanșatoarelor. **Capacități Non-funcționale** Arhitectura Sistemului se aliniază la necesitățile Beneficiarul ce țin de flexibilitatea și mentenabilitatea sistemului. Sistemul reprezintă o arhitectură deschisă, modulară, bazată pe componente interoperabile. Aceste principii sunt vizibile la toate nivelele arhitecturii sistemului. Arhitectura sistemului este de tipul client-server, organizată în 3 nivele verticale (utilizator, aplicație, date) , divizate clar, astfel încât fiecare nivel superior depinde doar de nivelul său inferior. Comunicarea între toate componentele sistemului se face securizat, utilizând în acest scop interfețele interne ale componentelor sistemului Sistemul**.** Nivelul de prezentare este responsabil pentru asigurarea interacțiunii utilizatorului cu funcțiile de business ale Sistemului. Acest nivel de arhitectură gestionează modul în care utilizatorii accesează și utilizează funcțiile Sistemului atât în scop de business, cât și în scop administrativ. Sistemul urmează este accesat doar de către utilizatorii autorizați. Suplimentar, Sistemul comunica cu alte sisteme ale Beneficiarul prin interfețe externe (cerințe relevante sunt stabilitate la capitolul „Interoperabilitate”). Aplicația client poate fi rulată în medii de operare standard sau cu configurări minime din partea Beneficiarului (ex. doar soft standard de sistem).

Aplicația client va putea fi rulată în medii de operare standard sau cu configurări minime din partea Beneficiarului (ex. doar soft standard de sistem). Nivelul de prezentare nu va implementa reguli de business, cu excepția validării datelor de intrare. Nivelul de date La acest nivel de arhitectură sunt stocate și accesate datele a sistemului. Datele sunt accesibile prin intermediul serviciilor de gestiune a bazelor date (SGBD). La nivelul SGBD sunt stabilite regulile de integritate pentru date. Nivelul de date trebuie să asigure că datele vor putea fi accesate doar de entitățile autorizate, iar datele vor rămâne integre și corecte. Nivelul de date trebuie să asigure datele necesare sistemului pentru furnizarea funcționalităților și serviciilor de business solicitate de Beneficiar. Următoarele sunt cerințele aferente arhitecturii pentru nivelul de date. Datele nu vor fi stocate redundant, relațiile de integritate intre date vor fi complet și corect definite și implementate, pornind de la rolul de business al datelor. Modelul de date trebuie să asigure posibilitatea migrării datelor din sistemele existente în cadrul Beneficiarul în sistemul. Datele sistemului trebuie să poată fi accesate doar prin intermediul componentelor conținute de nivelul de business logică. Arhitectura de date trebuie să fie optimizată din punct de vedere al accesării datelor pentru efectuare tranzacții și pentru analize și raportări. Fiecare înregistrare a obiectului informațional va avea un număr de identificare unic. Algoritmul de atribuire a numărului de identificare va fi configurabil în cadrul sistemului. Arhitectura sistemului trebuie să asigure integritatea și corectitudinea datelor la accesarea și modificarea datelor simultan de mai multe entități (utilizatori, procese interne, aplicații externe). Nivelul tehnologic La acest nivel de arhitectură sunt plasate componentele soft și hard necesare pentru rularea componentelor sistemului. Nivelul tehnologic al arhitecturii trebuie să asigure disponibilitatea și accesibilitatea componentelor sistemului. Următoarele sunt cerințele aferente arhitecturii pentru nivelul tehnologic. Arhitectura tehnologică a sistemului trebuie să dețină un nivel înalt de	Nivelul de prezentare nu implementează reguli de business, cu excepția validării datelor de intrare. Nivelul de date. La acest nivel de arhitectură sunt stocate și accesate datele a sistemului. Datele sunt accesibile prin intermediul serviciilor de gestiune a bazelor date (SGBD). La nivelul SGBD sunt stabilite regulile de integritate pentru date. Nivelul de date asigură că datele vor putea fi accesate doar de entitățile autorizate, iar datele vor rămâne integre și corecte Nivelul de date asigură datele necesare sistemului pentru furnizarea funcționalităților și serviciilor de business solicitate de Beneficiar. Următoarele sunt capacități aferente arhitecturii pentru nivelul de date. Datele nu sunt stocate redundant, relațiile de integritate intre date sunt complet și corect definite și implementate, pornind de la rolul de business al datelor. Modelul de date asigură posibilitatea migrării datelor din sistemele existente în cadrul Beneficiarul în sistemul. Datele sistemului sunt accesate doar prin intermediul componentelor conținute de nivelul de business logică. Arhitectura de date este optimizată din punct de vedere al accesării datelor pentru efectuare tranzacții și pentru analize și raportări. Fiecare înregistrare a obiectului informațional are un număr de identificare unic. Algoritmul de atribuire a numărului de identificare este configurabil în cadrul sistemului. Arhitectura sistemului asigură integritatea și corectitudinea datelor la accesarea și modificarea datelor simultan de mai multe entități (utilizatori, procese interne, aplicații externe). **Nivelul tehnologic** La acest nivel de arhitectură sunt plasate componentele soft și hard necesare pentru rularea componentelor sistemului. Nivelul tehnologic al arhitecturii asigură disponibilitatea și accesibilitatea componentelor sistemului. **Capacități aferente arhitecturii tehnologice**. Arhitectura tehnologică a sistemului deține un nivel înalt de rezistență la căderi, nu conține puncte singulare de cădere (SPOF).

rezistență la căderi, să nu conțină puncte singulare de cădere (SPOF). Arhitectura tehnologică trebuie să asigure utilizarea rațională și balansată a resurselor de procesare. Sistemul trebuie sa dispună de un mecanism de monitorizare și notificare în caz de abateri de la regimul standard de funcționare a posturilor de supraveghere Platforma tehnologică Platforma tehnologică este formată din totalitatea componentelor soft și hard necesare pentru a asigura mediul de operare în care va rula aplicația Componentele sistemului trebuie să fie independente de platforma tehnologica pe care rulează (cu excepția cazurilor când asemenea cerințe rezultă explicit din acest Caiet de sarcini). Arhitectura sistemului trebuie să fie optimizată pentru rularea în medii de tipul cloud computing. Caracteristici ale unui sistem cu arhitectură orientată spre implementare în Cloud, sunt: conștient de latență, conștient de căderi de componente, paralelizabil, conștient de utilizarea resurselor. Tehnologiile prezente la nivelul platformei tehnologice trebuie să fie omogene (număr minim de tehnologii diferite, ex. diferite sisteme de operare pentru middleware și data base). Sistemul trebuie sa fie proiectat si implementat pentru tehnologii de tip web, utilizind patern-uri si framework-uri deschise. Ofertantul va indica în oferta sa informație completă privind platformele tehnologice suportate de aplicația sa. Interoperabilitate Interoperabilitatea sistemului reprezintă caracteristica acestora de a comunica cu alte aplicații. Arhitectura de sistem stabilește interfețele ce trebuie să existe intre Sistem și alte sisteme ale Beneficiarului. La acest punct sunt stabilite cerințele privind caracteristicile de interoperabilitate ale sistemului solicitate de Beneficiar. Toate interfețele sistemului trebuie să fie bazate pe standarde deschise. Toate fluxurile de mesaje între Sistem și entități externe se vor realiza cu utilizarea standardelor deschise. Toate interfețele sistemului furnizate vor putea interacționa cu aplicațiile externe atât în regim real, cat și în regim off-line. Interfețele sistemului furnizate vor permite cuplarea slaba cu aplicațiile externe (comunicare în baza de mesaje).	Arhitectura tehnologică asigură utilizarea rațională și balansată a resurselor de procesare. Sistemul dispune de un mecanism de monitorizare și notificare în caz de abateri de la regimul standard de funcționare a posturilor de supraveghere **Platforma tehnologică** Platforma tehnologică este formată din totalitatea componentelor soft și hard necesare pentru a asigura mediul de operare în care va rula aplicația Componentele sistemului sunt independente de platforma tehnologica pe care rulează . Arhitectura sistemului este optimizat pentru rularea în medii de tipul cloud computing cu caracteristici ale unui sistem cu arhitectură orientată spre implementare în Cloud (conștient de latență, conștient de căderi de componente, paralelizabil, conștient de utilizarea resurselor). Tehnologiile prezente la nivelul platformei tehnologice sunt omogene cu număr minim de tehnologii diferite. Sistemul este proiectat si implementat pentru tehnologii de tip web, utilizind patern-uri si framework-uri deschise. Platformele de baza sunt Microsoft Windows și Linux. Vor fi folosite platforme de calcul, analitica, baze de date, stocare, securitate etc. Fiecare etapa de formare a softului va fi coordonata cu beneficiarul si reglementată sub cerințele acestuia. Posibilitatea extinderii funcționalității controlului, recunoașterii, observării prin conectarea unor module software și / sau hardware suplimentare care nu înrăutățesc caracteristicile operaționale, tehnice și metrologice ale complexului și nu încalcă conformitatea cu cerințele acestor condiții tehnice. **Interoperabilitate** Interoperabilitatea sistemului reprezintă caracteristica acestora de a comunica cu alte aplicații. Arhitectura de sistem stabilește interfețele ce există intre Sistem și alte sisteme ale Beneficiarului. La acest punct sunt stabilite cerințele privind caracteristicile de interoperabilitate ale sistemului solicitate de Beneficiar. Toate interfețele sistemului se bazează pe standarde deschise. Toate fluxurile de mesaje între Sistem și entități externe se realiza cu utilizarea standardelor deschise.

Sistemul va deține interfețe standard pentru exportul datelor în cadrul instrumentelor de tipul Data Warehouse. Sistemul va deține posibilitatea de a crea mesaje email conform formularelor prestabilite și de a le expedia către destinatarii indicați prin intermediul serverului de posta electronica setat în configurațiile sistemului. Securitate Sistemul trebuie să permită un control adecvat asupra riscurilor de securitate a informației aferente utilizării. Măsurile de securitate implementate trebuie să fie aliniate la politicile de securitate aprobate în cadrul MAI. Arhitectura sistemului trebuie să fie concepută prin aplicarea unei abordări de tipul „Secure by design" (Securitate prin design). Arhitectura de securitate a sistemului trebuie să fie documentată la nivel tehnic. Documentația va conține descris modelul de securitate implementat, componentele prezente și rolul fiecărei componente din punct de vedere al securității. Toate credențialele de acces utilizate de aplicație trebuie să fie configurabile în interfețele administrative. Sistemul nu va conține credențiale de acces hard-coded. Sistemul nu va stoca la nivelul componentelor sale (în baza de date, fișiere de configurație) credențiale de acces în formă deschisă. Autentificare Sistemul va permite accesarea funcțiilor Sistemului doar după autentificarea cu succes a utilizatorului. Sistemul va oferi suport pentru cel puțin următoarele metode de autentificare: În bază de ID și parolă, prin intermediul serviciului electronic guvernamental de autentificare și control al accesului – Mpass Sistemul va permite înregistrarea utilizatorilor și a informației de profil aferentă acestora (ex. ID, parola, nume, prenume, email, etc.). Parolele utilizatorilor trebuie să fie protejate în cadrul sistemului. Metoda de protejare a parolelor trebuie să asigure imposibilitatea interceptării, deducerii sau recuperării acestora. Sistemul va permite definirea și implementarea seturilor de politici de utilizare a parolelor. Politicile trebuie să permită setarea cerințelor cel puțin pentru: complexitatea parolei, obligativitatea schimbării parolei, durata de viață a parolei. Sistemul va permite blocarea, dezactivarea sau suspendarea conturilor utilizatorilor la nivel de aplicație. Autorizare Sistemul va permite gestiunea granulară a drepturilor de acces	Toate interfețele sistemului furnizate interacționează cu aplicațiile externe atât în regim real, cat și în regim off-line. Interfețele sistemului furnizate permite cuplarea slaba cu aplicațiile externe (comunicare în baza de mesaje). Sistemul deține interfețe standard pentru exportul datelor în cadrul instrumentelor de tipul Data Warehouse. Sistemul deține posibilitatea de a crea mesaje email conform formularelor prestabilite și de a le expedia către destinatarii indicați prin intermediul serverului de posta electronica setat în configurațiile sistemului. **Securitate** Sistemul permite un control adecvat asupra riscurilor de securitate a informației aferente utilizării. Măsurile de securitate implementate sunt aliniate la politicile de securitate aprobate în cadrul MAI. Arhitectura sistemului este concepută prin aplicarea unei abordări de tipul „Secure by design" (Securitate prin design). Arhitectura de securitate a sistemului este documentată la nivel tehnic. Toate datele formate si transmise vor avea semnătură digitală. Ce folosește confuziționarea codului,chei de criptare, codul pentru server,modul pentru controlul fascicolului de date prin SHA 256, securitatea softului și informației împotriva intervenției neprevăzute, securitatea datelor pentru fiecare utilizator separat legate de login/ pasword și delimitarea pe nivelul de acces. Acces sigur la sistem și organizarea lucrărilor cu mai mulți utilizatori cu diferențierea drepturilor de acces pentru diferite categorii de utilizatori. Toate credențialele de acces utilizate de aplicație sunt configurabile în interfețele administrative. Sistemul nu conține credențiale de acces hard-coded. Sistemul nu stochează la nivelul componentelor sale (în baza de date, fișiere de configurație) credențiale de acces în formă deschisă. **Autentificare** Sistemul permite accesarea funcțiilor Sistemului doar după autentificarea cu succes a utilizatorului. Sistemul oferă suport pentru cel puțin următoarele metode de autentificare: În bază de ID și parolă, prin intermediul serviciului electronic guvernamental de autentificare și control al accesului – Mpass Sistemul permite înregistrarea utilizatorilor și a informației de profil aferentă acestora (ex. ID, parola, nume, prenume, email, etc.).

Metoda de autorizare în cadrul sistemului se va baza pe principiul „este interzis tot ce nu este explicit permis”. Sistemul va deține vizualizări și rapoarte privind drepturile de acces existente în Sistem. Auditul și monitorizarea de securitate Sistemul va deține componente de audit ce vor colecta și gestiona centralizat înregistrările de audit la nivelul fiecărui modul Sistemul. Înregistrările de audit nu vor conține informație de business confidențială (ex. parole introduse la încercările eșuate). Erorile ce pot apărea la fixarea înregistrărilor de audit nu trebuie să afecteze funcționarea normală a sistemului. Componenta de audit va utiliza ceasul de sistem setat la nivelul sistemului de operare în care rulează componenta de audit. Activități de schimbare stări și responsabili înregistrări vor fi jurnalizate. Sistemul va deține instrumente comode pentru accesarea și procesarea evenimentelor log înregistrate, inclusiv filtrarea înregistrărilor de audit după orice câmp deținut și exportul acestora în format uzual. Instrumentele de audit ale sistemului vor putea fi utilizate și în scopul importului arhivelor cu fișiere de audit pentru activități de analiza ocazionale.	Parolele utilizatorilor sunt protejate în cadrul sistemului. Metoda de protejare a parolelor asigură imposibilitatea interceptării, deducerii sau recuperării acestora. Sistemul permite definirea și implementarea seturilor de politici de utilizare a parolelor. Politicile permit setarea cerințelor pentru: complexitatea parolei, obligativitatea schimbării parolei, durata de viață a parolei. Sistemul permite blocarea, dezactivarea sau suspendarea conturilor utilizatorilor la nivel de aplicație. **Autorizare** Sistemul permite gestiunea granulară a drepturilor de acces Metoda de autorizare în cadrul sistemului se bazează pe principiul „este interzis tot ce nu este explicit permis”. Sistemul deține vizualizări și rapoarte privind drepturile de acces existente în Sistem. **Auditul și monitorizarea de securitate** Sistemul deține componente de audit ce colectează și gestionează centralizat înregistrările de audit la nivelul fiecărui modul Sistemul. Înregistrările de audit conține informație de business confidențială (ex. parole introduse la încercările eșuate). Erorile ce pot apărea la fixarea înregistrărilor de audit nu afecteze funcționarea normală a sistemului. Componenta de audit utilizează ceasul de sistem setat la nivelul sistemului de operare în care rulează componenta de audit. Activități de schimbare stări și responsabili înregistrări vor fi jurnalizate. Sistemul deține instrumente comode pentru accesarea și procesarea evenimentelor log înregistrate, inclusiv filtrarea înregistrărilor de audit după orice câmp deținut și exportul acestora în format uzual. Instrumentele de audit ale sistemului vor putea fi utilizate și în scopul importului arhivelor cu fișiere de audit pentru activități de analiză ocazionale.

Administrator
Cornel Ababii